Säker digitalisering med NIS2

Ciscos vägledning runt NIS2-direktivet

Radar.

cisco

Förord

Den här rapporten riktar sig till verksamhetsledare och beslutsfattare med syfte att ge vägledning och insikter om en säker digitalisering. Rapporten påvisar potentialen och värdet av en hög digitaliseringstakt i samhället, redogör för den ökade hotbilden och risken mot vår fortsatta digitala utveckling och konkurrenskraft, samt diskuterar hur det nya EU-direktivet NIS2 svarar upp mot detta genom att utgöra en grund för en bred säker digitalisering som kommer hela samhället till gagn.

Därtill så bidrar rapporten med ett branschperspektiv på NIS2-direktivet genom en djupare inblick och analys i fyra branscher och sektorer: bank och finans, kritisk infrastruktur, regioner samt kommuner. I denna del berörs respektive bransch eller sektors olika förutsättningar, utmaningar samt generella mognadsgrad kring att hantera en implementering av NIS2. Dessutom lyfts även ett antal konkreta ”call-to-action” per sektor som hjälp på vägen. Dessa utvalda branscher har olika erfarenhet och vana vid att arbeta med regulatoriska krav, vilket gör det intressant att jämföra dem och dra lärdom från deras respektive perspektiv, även för den verksamhet som befinner sig inom en annan sektor eller bransch.

Slutligen presenteras en enkel vägledning för att komma i gång med en implementering av NIS2-direktivet genom konkreta exempel på aktiviteter och förmågor som kan bidra till att uppnå och bibehålla en efterlevnad av NIS2 – för en fortsatt säker digitaliseringsresa.

Rapporten är framtagen i ett samarbete mellan Cisco och Radar Group, där nordiska specifika data tillsammans med öppna och tillgängliga data har analyserats med djup industriell expertis och erfarenhet inom IT-landskapet. Detta har kombinerats med insikter från djupintervjuer som har genomförts med respondenter från olika verksamheter inom både privat och offentlig sektor.

Foto omslag: Remus Kotsell, iStockphoto

Innehåll

1. Vikten av en säker digitalisering

1.1 Digitalisering som motor för sveriges utveckling

Digitaliseringen och den digitala transformationen har blivit viktiga verktyg inom alla verksamheter, såväl privata som offentliga. De digitala verktygen hjälper verksamheter att möta köpare och användares nya behov, skapa helt nya arbetssätt, processer, tjänster eller erbjudanden, samt att sänka kostnader eller effektivisera verksamheten. Digitaliseringen började redan på 1940-talet genom ersättandet av analog teknik med digital teknik och samhället står nu på randen till en bredskalig utrullning av datadriven digitalisering med stöd av AI. Nya digitala värden skapas genom att koppla samman människor med olika applikationer och datakällor och automatisera dessa flöden. Digitaliseringen har varit en viktig del i att stärka den svenska konkurrenskraften, ekonomin och välfärden.

Ett sätt att bedöma styrkan i Sveriges digitaliseringsmotor är att titta på Europeiska kommissionens index för digitalisering kallat indexet för digital ekonomi och digitalt samhälle (DESI)[8]. DESI-indexet rangordnar medlemsländernas digitaliseringsmognad enligt fyra kriterier: humankapital förklarat som medborgarnas digitala förmåga, konnektivitet, integrering av digital teknik, samt digitaliseringsnivån i offentlig sektor. För 2022 års mätning placerar sig Sverige på en fjärdeplats bland EU:s 27 medlemsländer. Fjärdeplatsen visar att Sverige har en stark position inom Europa vad gäller digital förmåga, men detta är en placering sämre än föregående mätning. Det är viktigt att fortsätta hålla ett starkt fokus på digitalisering och att politiker skapar förutsättningar för nödvändiga digitala satsningar för att uppnå den uttalade ambitionen om att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

Indexet för digital ekonomi och digitalt samhälle 2022 (DESI Index 2022)

Topp 5 DESI Index 2022	DESI Kriterier	Sveriges placering per kategori
1. Finland	**Medborgares digitala förmåga**	**4:e Plats –** Medborgares digitala förmåga
2. Danmark	**Konnektivitet**	**9:e Plats –** Konnektivitet
3. Nederländerna	**Integrering av digital teknik**	**3:e Plats –** Integrering av digital teknik
4. Sverige	**Digitala offentliga tjänster**	**9:e Plats –** Digitala offentliga tjänster
5. Irland		

Sverige och svenska verksamheter har kommit långt inom digitaliseringen, och denna rapport kommer att handla om värdet av att fortsätta denna utveckling, men även vikten av att genomföra digitalisering med ett integrerat säkerhetsfokus. För att vara en vinnare i framtiden kommer det att krävas kunskap och förmåga kring att genomföra säker digitalisering.

1.2 Den digitala accelerationen

Det uppskattas att den globala pandemin som inleddes 2019 accelererade digitaliseringstakten med 3–4 år och är sedan dess fortsatt ökande. De aktörer som historiskt fokuserat på digitalisering under kriser, såsom den finansiella krisen 2008 eller den globala pandemin, klarade sig bättre eller kom till och med starkare ur kriserna genom att använda digitaliseringen som ett verktyg för ökad uthållighet och flexibilitet. De verksamheter som lyckades bäst hade en förmåga att bibehålla sina digitala initiativ eller påbörja nya under kriserna.

Prestation hos digitalt ledande bolag jämfört med genomsnitt i samma bransch13

x1,9	x1,5
Ökad tillväxt efter 10 år (faktor)	**Ökad lönsamhet efter 3 år (faktor)**

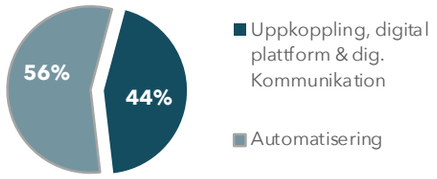
Många verksamheter ser nu ser över sina verksamhets- och affärsmodeller i syfte att undersöka hur dessa kan stärkas genom digitala initiativ. Så många som sex av tio säger att de behöver öka det digitala inslaget i sina affärsmodeller inom en femårsperiod för att de fortsatt skall vara relevanta.

Som ett resultat av digitaliseringen skapas mer data och världen befinner sig nu i en data-genereringstakt där den globala mängden data fördubblas var artonde månad. Takten har aldrig varit så hög som den är nu och den förväntas öka ytterligare. Till följd av denna utveckling har EU börjat kommunicera om den nya dataekonomin och dess betydelse. Redan år 2025 förväntas den nya dataekonomin utgöra över fyra procent av EU:s samlade BNP[34], vilket är upp knappt två procentenheter sedan 2019. Det gör den växande dataekonomin till en avgörande och kritisk komponent i det europeiska välfärdssystemet.

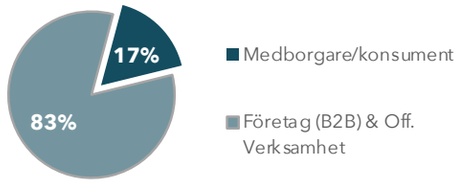
1.3 Värdet av digitaliseringen

Den samlade teoretiska potentialen av en säker digitalisering i Sverige, inom både privat och offentlig sektor, uppskattas till mer än 800 miljarder SEK[16] från 2025 och framåt, vilket är mer än 15 procent av 2021 års samlade BNP. För att sätta siffran 800 miljarder i en kontext så innebär det att det potentiella värdet motsvarar två av de enskilt största BNP tillskotten; den samlade tillverkningsindustrin (15 procent av svenskt BNP) eller den samlade kommunala verksamheten (14 procent av svenskt BNP)[24].

Teknisk fördelning (%) av potentialen av säker digitalisering[16] (>800 MSEK)



Målgruppsfördelning (%) av potentialen av säker digitalisering[16] (>800 MSEK)



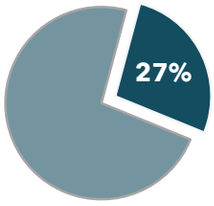
En analys av möjligheterna att kapitalisera på denna stora potential i samhället visar att det är lika viktigt att hålla fokus på att automatisera (56 procent) sin verksamhet som att tillföra mer modern teknik och digitala plattformar (44 procent). Vad som är ännu mer intressant är att det är inom och mellan verksamheter som den största potentialen ligger (83 procent), jämfört med att digitalisera interaktionen med medborgaren (offentlig verksamhet) eller konsumenten (företag) (17 procent), även om digitalisering i denna interaktion även kan ge andra viktiga fördelar.

Från ett övergripande nationellt samhällsperspektiv är det potentiella värdet av digitaliseringen intressant ur två aspekter:

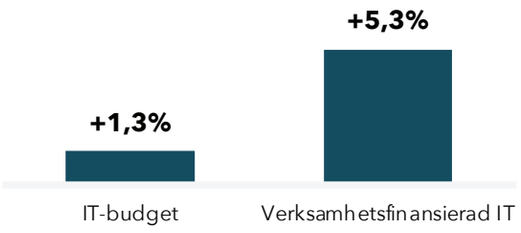
- **Den aggregerade potentialen av säker digitalisering** är så pass omfattande att Sverige som nation måste fokusera på den. Om vi kan fånga stora delar av potentialen skapar det förutsättningar för ett nytt, bättre och mer robust Sverige.
- **Potentialen i förhållande till det övriga värdeskapandet** i samhället är så pass stor att den kommer medföra stora omställningar, inte bara för individ och verksamhet, utan i hela samhället. Det ligger därför i nationens och samhällets intresse att dra nytta av denna potential för att maximera de positiva effekter som finns att hämta.

Det här har verksamheter och organisationer börjat förstå och idag blir IT och digitala lösningar ett alltmer naturligt inslag och en möjliggörare för att skapa nya värden i verksamheten. Ett sätt att mäta denna utveckling är att studera hur stor andel av den totala IT-budgeten som finansieras av verksamheten, det vill säga där IT-investeringar beslutas av verksamhetschefer, jämfört med IT-budgeten som oftast ägs av den centrala IT-organisationen. Under 2023 bedöms 27 procent av den totala IT-budgeten i Sverige vara verksamhetsfinansierad, vilket är en rekordnotering[22]. Andelen verksamhetsfinansierad IT växer dessutom i högre takt jämfört med den totala IT-budgeten. Slutsatsen blir därmed att digitalisering drivs mer och mer av verksamheten än IT-avdelningen. Denna omdisponering ställer nya krav och den ökande andelen IT och digitala verktyg inom kärnverksamheten ökar även behovet av en säker digitalisering.

Verksamhetsfinansierad IT som andel av totala IT kostnader 2023[22]

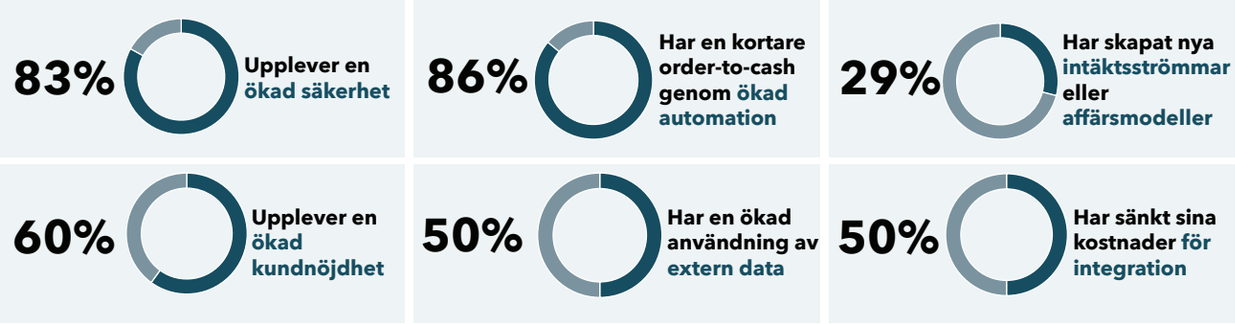


Årlig tillväxttakt av IT-budget 2023[22]



Den digitala accelerationen möjliggör för helt nya affärsmodeller och har tydligt påverkat hur verksamheter konsumerar IT. Det sker en snabb tillväxt av digitala plattformar där IT kan konsumeras som tjänst (as-a-service) med en snabbhet, enkelhet och flexibilitet som passar många verksamheter. De många fördelarna med den lättkonsumerade plattformstekniken gör att tillväxttakten är flera gånger högre än för IT-budgeten 2023[22]. Det ställer dock krav på helt nya domänkunskaper inom både verksamheten och den centrala IT-organisationen för att bedriva en säker digitalisering med den nya plattformtekniken och fortfarande är mognadsgraden inom de flesta verksamheter relativt låg. För de som kommit långt på sin digitaliseringsresa finns däremot tydliga affärsvärden att påvisa.

En studie av olika nordiska verksamheters förmåga att skapa värde av data visade att de verksamheter som investerade i digitala plattformar påvisade en högre lönsamhet och/eller effektivitet än andra med liknande förutsättningar[15]. Därtill visade studien att de verksamheter som lyckades bäst med att utvinna affärsnytta ur sin data uppvisade följande värden:



2. Hotet mot digitaliseringen

Samhället står just nu inför ett dilemma. Å ena sidan finns en bred insikt om potentialen och nyttan av digitalisering inom samhället och digitaliseringstakten accelererar. Samtidigt medför samma digitalisering att hotbilden ökar. Risken för cyberangrepp är dels ett reellt hot mot den fortsatta digitala utvecklingen, men även mot samhället i stort för upprätthållanden av vår välfärd och för nationens ekonomiska stabilitet. Kostnaderna för att drabbas av cyberattacker och incidenter ökar, men ännu större är den potentiella indirekta kostnaden av en osäker digitalisering som bidrar till att minska trovärdigheten och tilliten till samhällets och företagens tjänster. Cybersäkerhetsfrågan har blivit kritisk att hantera för både nationer och verksamheter för att säkra vår fortsatta utveckling, konkurrenskraft och för att skydda viktiga värden och rättigheter.

Samtidigt som potentialen med digitalisering onekligen är stor, så finns det även en betydande risk för förlorade värden av att försumma eller genomföra en bristfällig och icke säker digitalisering. En utebliven eller dåligt genomförd digitalisering i Sverige kan i kontrast medföra en inbromsning och ett årligt tapp av BNP uppskattat till 70 miljarder SEK[20] (ca en procent av BNP).

Exempel på effektförluster som en bristfällig digitalisering kan skapa och som påverkar samhället, vårt BNP och vår välfärd negativt kan vara:

Effektivitetsförlust	**Förlorad konkurrenskraft**	**Försämrad medborgarservice**
Ökade kostnader	**Förlorade intäkter**	**Ökad sårbarhet**
Misstroende & förlorad relation	**Försämrad kommunikation**	**Minskad tillit**
Utanförskap	**Förlorade skatteintäkter**	**Försämrad välfärd**

2.1 Det nya hotlandskapet

Det geopolitiska läget påverkar den globala utvecklingen och får tydliga effekter på vårt nordiska IT-ekosystem. Under 2023 väntas utvecklingen och det osäkra omvärldsläget att fortsätta, där en av de stora frågorna är de ökade spänningarna mellan stormakter och allianser. Handelskrig, jakt

på teknisk dominans och territoriella anspråk kommer att fortsätta påverka den internationella arenan. I Säpos årsrapport framgår det att Ryssland och andra auktoritära stater som Kina och Iran har blivit alltmer offensiva i sitt agerande och säkerhetshotande aktiviteter nu pågår ständigt[27]. I kombination med en ökande digitalisering kommer cybersäkerhet och informationsintegritet att fortsatt kopplas till den geopolitiska utvecklingen.

Cyberattacker är bland de snabbast växande formerna av brottslighet

Som en högt digitaliserad ekonomi är den förhöjda hotbilden tydlig i Sverige. Den ökade sammanlänkningen av vår digitala infrastruktur och vårt starka fokus på digitalisering medför en ökad sårbarhet och ökande attackytor. Därtill påverkas vi av det försämrade säkerhetsläget, vår ansökan till NATO, samt en omfattande kompetensbrist på IT-säkerhetsexperter. Cyberattacker är bland de snabbast växande formerna av brottslighet, och blir alltmer komplext och kostsamt att skydda sig mot[6]. Vi står idag inför ett systematiskt säkerhetshot drivet av aktörer med politiska, militära eller ekonomiska intressen.

På samma sätt som den tekniska utvecklingen kan skapa värde för verksamheter och samhället möjliggör den även för mer sofistikerade och avancerade metoder för att utföra cyberattacker. Därtill har cyberbrottslingarnas förmåga och intresse för attacker mot de digitala leverantörskedjorna ökat, vilket får stora effekter genom hela IT-ekosystemet. Sedan den uppmärksammade attacken mot SolarWinds i slutet av 2020 har allt fler hotaktörer insett potentialen i attacker mot leverantörskedjor, vilka steg från mindre än 1 procent av intrången 2020 till 17 procent 2021, och har sedan dess fortsatt att öka[3].

2.2 Aktörer och drivkrafter

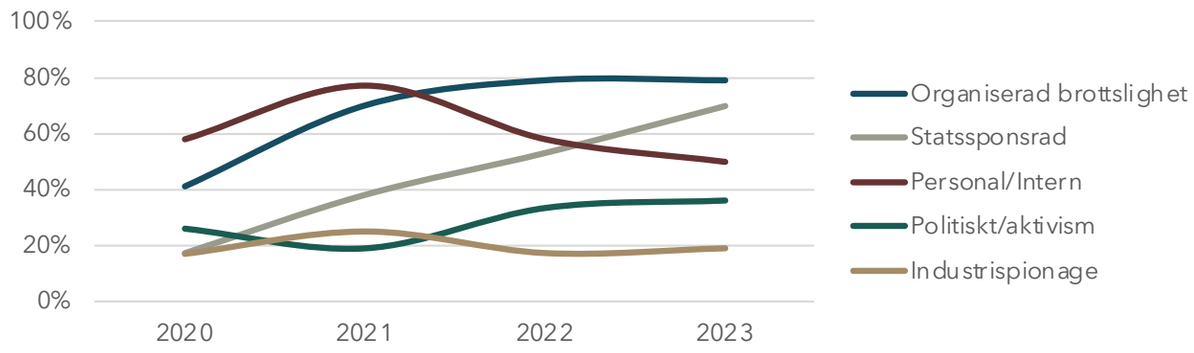
Cyberhoten som riktas mot svenska aktörer och intressen är mångfacetterade och kommer ifrån olika typer av hotaktörer med olika drivkrafter.

Statliga aktörer eller statssponsrade aktörer är ett stort hot då de ofta har stora resurser och förmågor och en hög uthållighet för att bedriva destabiliserande eller skadliga aktiviteter i ett mer långsiktigt perspektiv. Utöver att åsamka direkt skada kan de hänge sig åt aktiviteter som exempelvis underrättelseverksamhet och påverkanskampanjer med syfte att undergräva förtroendet för samhällets institutioner eller påverka det svenska samhället enligt den egna nationens intressen.

Kriminella aktörer drivs primärt av ekonomiska intressen och är snabba på att anamma ny teknologi eller nya metoder för att hitta nya sätt att tjäna pengar. Vilka mål denna aktör riktar in sig på är till skillnad från de statliga aktörerna inte det primära, utan högsta möjliga avkastning till minsta möjliga risk styr vem som blir utsatt. Organisatoriskt börjar de mer likna startups än kriminella gäng i och med tjänstefieringen av cyberbrott, en ökande grad av specialisering och en växande infrastruktur för att bedriva den brottsliga verksamheten.

Hacktivister är individer eller grupperingar drivna av ideologiska motiv eller politiska intressen. Denna typ av aktör bedriver ofta ”enklare” aktiviteter som DDoS (överbelastningsattacker) som inte åsamkar permanent skada utan syftar till att skapa uppmärksamhet. Denna typ av attacker påverkar tillgängligheten vilket likväl bidrar till att skada förtroendet för de verksamheter som drabbas.

Svenska verksamheters upplevda hotbild[21]



De kriminella aktörerna upplevs som det största hotet av svenska verksamheter, tätt följt av de statssponsrade aktörerna som är den hotvektor som ökat kraftigast de senaste åren. Upplevelsen av det interna hotet, vilket kan härstamma från både medvetna och omedvetna handlingar, ser en minskande andel jämfört med de externa hoten. Det är förståeligt att de externa hoten har ett ökat fokus givet det osäkra geopolitiska läget och den senaste tidens uppmärksammade cybersäkerhetsincidenter. Det är dock viktigt att även fortsätta hålla fokus på att utbilda och stärka förmågan hos den interna personalen då de står för en betydande andel av upptäckta incidenter.

2.3 Verksamheternas utmaningar

Den digitala accelerationen skapar utmaningar och hot som verksamheter behöver hantera och skydda sig mot genom ett systematiskt säkerhetsarbete. Nedan följer några av de vanligaste cyberbrotten som drabbar verksamheter och samhället just nu:

Indexet för digital ekonomi och digitalt samhälle 2022 (DESI Index 2022)		
Ransomware	Digitala tillgångar eller data blir kapade och en lösensumma utkrävs.	Vanligt förekommande Ökande trend
Malware	Skadlig kod implementeras och hotar säkerhetsklassning, integritet eller tillgång till data eller applikationer.	Vanligt förekommande Ökande trend
Social Engineering	Utnyttjande av personalens okunskap eller misstag. Syftar till att få tillgång till verksamhetens digitala landskap, data eller tjänster. Ny teknologi gör tillvägagångssätten mer sofistikerade.	Vanligt förekommande Stabil trend
Dataintrång	Syftar till att få ej auktoriserad tillgång till data i syfte att kontaminera, utnyttja den eller låsa för användning.	Vanligt förekommande Ökande trend
Hot mot tillgänglighet	Överbelastningsattack (så kallad DDoS) som syftar till att stoppa digitala funktioner eller tjänster. Metoden har industrialiserats och spridits mer under senaste tiden. Har även använts som verktyg i det pågående kriget i Europa.	Vanligt förekommande Ökande trend
Desinformationskampanjer	Nyttjande av sociala medier eller digitala medieplattformar för att sprida desinformation. Används av statliga eller statssponsrade aktörer för att skada och påverka verksamheter eller nationer och underblåsa splittringar.	Från låg nivå men starkt ökande Ökande trend
Attack mot leverantörskedja	Syftar till att åsamka skada hos både kund och leverantör och får snabbt kaskadeffekter. Leder ofta till stöld av data eller spridning av Ransomware.	Från låg nivå men ökande Ökande trend

De upplevda utmaningarna återspeglas även i IT-beslutsfattares viktigaste IT-strategiska prioriteringar för året. Det är ett fortsatt stort fokus på digitalisering, men där vikten av att genomföra en säker digitalisering genom ett ökat säkerhetsfokus tydliggjorts. Värdet av digitalisering har blivit allt tydligare och nu följer även en ökad förståelse för att säkerhetsfrågan behöver prioriteras för att säkra potentialen av digitaliseringen[22].

IT-beslutsfattares viktigaste prioriteringar för året[22]:

- **Strategisk efterlevnad av cybersäkerhetskrav**
  När kärnverksamheten blir alltmer digitaliserad och verksamheten står för en ökad andel av IT-investeringarna får säkerhetsfrågan ett högre strategiskt fokus.
- **Digitalisering**
  Det finns ett stort fokus i både offentliga och privata verksamheter för fortsatt digitalisering för att utveckla nya operativa modeller och/eller affärsmodeller.
- **Kompetensutveckling inom cybersäkerhet**
  För att både möta den strategiska efterlevnaden av cybersäkerhet och samtidigt bibehålla fokus på en hög och hållbar digitaliseringstakt krävs helt nya kompetenser.

En av de viktigaste komponenterna i en organisations cybersäkerhets-förmåga och för att lyckas med en säker digitalisering är personalens grundläggande IT-säkerhetskompetens. Personal är inblandad i åtta av tio intrång och incidenter i Norden och spelar därmed en viktig roll inom cybersäkerhetsarbetet. Detta visar att det fortfarande finns ett stort behov av att höja organisationens generella cybersäkerhetskompetens som ett led i arbetet med att säkra digitaliseringen av verksamheten. Denna analys understöds av ENISA:s rapport från 2022 som visar att endast fyra av tio europeiska samhällskritiska verksamheter bedriver bred, strukturerad och kunskapslyftande cybersäkerhetsinitiativ i syfte att utbilda personalen[2].

2.4 Kostnader kopplade till en osäker digitalisering

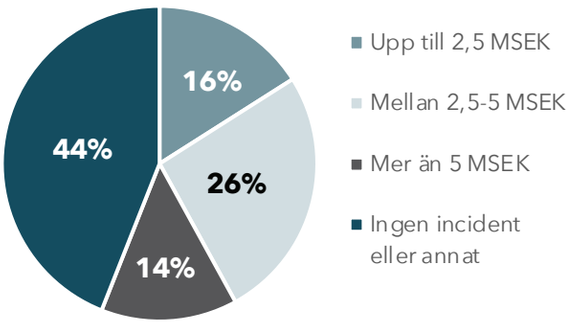
Inom EU lyfts de direkta och indirekta kostnaderna för den osäkra digitaliseringen som ett tydligt hot mot nationernas ekonomiska utveckling och mot välfärdssystemet. Genom att investera i övergripande strategier, initiativ och regulatoriska ramverk tillförs nu upp till 4,5 miljarder EUR för att förstärka digitaliseringen inom Europa[2].

Riskerna mot verksamheterna ökar när kostnaderna och konsekvenserna av att drabbas blir allt högre. På frågan vad den senaste stora incidenten medförde för direkta kostnader för verksamheten uppgav 40 procent av de tillfrågade att kostnaden översteg 2,5 miljoner SEK. Av de tillfrågade angav 14 procent att kostnaden varit mer är 5 miljoner SEK för den senaste incidenten[2].

EU:s säkerhetsorgan ENISA, uppskattar att mediankostnaden för en IT-incident i EU uppgår till 2 miljoner SEK under 2022. Det är en kostnads-fördubbling över ett år. De sektorer som just nu drabbas av de dyraste incidenterna är bank och finans samt hälso- och sjukvård.

Svenska verksamheter blir i högre utsträckning beroende av digital teknologi för att bedriva sin kärnverksamhet, vilket gör cybersäkerhet till en alltmer affärskritisk fråga att hantera. Många verksamheter saknar fortfarande kunskap om de egna skyddsvärdena[27], men i takt med att riskerna och kostnaderna blir allt högre och mer synliga kan vi se att säkerhetsfrågan får ett högre strategiskt fokus och ser ökande investeringar vilket är viktiga steg i rätt riktning[21].

Andelen (%) respondenter som anger direkt kostnad från den senaste incidenten[2]



3. Regulatoriska krav som möjliggörare för digitaliseringen

Införandet av en rad olika regulatoriska krav, däribland NIS2-direktivet, är ett politiskt svar på den ökade hotbilden. Det är tydligt att verksamheter och samhället inte lyckats höja sin cybersäkerhetsförmåga med samma fart och omfattning som digitaliseringen för att möta det nya hotet och stiftandet av lagar och förordningar är bland de enda verktyg som står till politikernas förfogande för att hantera detta.

Grunden till det nuvarande legislativa landskapet började läggas av EU redan för flera år sedan och innefattar en rad generella och specifika regulatoriska ramverk (för en mer detaljerad överblick över det regulatoriska landskapet, se bilaga A). Under 2020 lanserade EU en ny cybersäkerhetsstrategi som syftar till att öka Europas motståndskraft mot cyberhoten, skydda våra viktiga samhällsfunktioner och säkerställa att alla kan dra nytta av pålitliga digitala verktyg och tjänster. EU:s nya regelverk är bland de första på multilateral nivå som inte bara påverkar EU:s medlemsstater utan även andra länder som är beroende av den europeiska marknaden. Eftersom cyberhoten blir alltmer globala är det betydelsefullt för länder att samarbeta och utveckla gemensamma standarder för cybersäkerhet.

EU leder vägen

I jämförelse med resten av världen är det tydligt att EU har ett starkare fokus på reglering med syfte att stärka den inre marknaden. Regulatoriska krav ses som en proaktiv möjliggörare till stärkt konkurrenskraft, ekonomisk tillväxt och effektivt samarbete mellan medlemsländerna, samt med andra globala aktörer som erbjuder sina tjänster till den europeiska marknaden. Exempelvis adresserar flera av dessa ramverk hur data ska användas på ett säkert sätt inom unionen och vid utbyten med omvärlden för att uppnå så kallad digital suveränitet. En av förklaringarna till detta är att de flesta ledande tech-bolagen såsom Microsoft, Google, Meta och så vidare, återfinns utanför EU, vilket innebär att mängder av europeiska data hanteras inom bolag registrerade utanför Europa. I ett samhälle som använder och

nyttjar mer och mer data för välfärd och värdeskapande ökar således behovet av digital suveränitet. Detta driver utvecklingen av europeiska regulatoriska ramverk med syfte att skydda medlemsländerna som utgör en viktig marknad för dessa globala aktörer.

Att vara långt fram i det regulatoriska arbetet kan dessutom ha andra fördelar, då den europeiska lagstiftningen kan sätta en standard för resten av världen och ofta bli förlaga till annan lagstiftning. Exempelvis ledde introduktionen av GDPR till en global våg av integritets- och dataskydds-bestämmelser där GDPR användes som utgångpunkt i olika nationers utvecklingsarbete, däribland för Kinas egen version PIPL (the Personal Information Protection Law) samt USA:s CCPA (California Consumer Privacy Act).

Det digitaliserade samhället utgörs av en nära sammankopplad infrastruktur som Sverige är beroende av. Om en samhällskritisk sektor som exempelvis finans- eller energisektorn drabbas av störningar spiller det snabbt över på andra områden och verksamheter och får konsekvenser för hela samhället. En kedja är bara så stark som sin svagaste länk, vilket är hela grunden till de breda regulatoriska krav som nu introduceras. Det är viktigt att samhälls-kritiska verksamheter gemensamt höjer sin försvarsförmåga, inte bara för att skydda den egna verksamheten, utan som ett led i att säkra hela kedjan och därmed samhällets motståndskraft.

3.1 Från NIS till NIS2

I EU:s nya cybersäkerhetsstrategi beslutades om en revidering av det tidigare NIS-direktivet (säkerhet i nätverk och informationssystem). Anledningen var att hantera de brister som framkommit sedan imple-menteringen av NIS och samtidigt uppdatera direktivet för att bättre möta dagens och morgondagens utmaningar och risker i vårt digitaliserade samhälle[6].

Några av problemen med den tidigare lagstiftningen innefattade tydliga brister i tillämpningen av direktivet samt ineffektiv tillsyn[7]. Därtill fanns det stora skillnader mellan medlemsländerna i synen på vad som ansågs vara samhällsviktiga tjänster som ledde till att liknande verksamheter i olika länder mötte olika krav vilket bidrog till att hämma konkurrensen på den inre marknaden.

”NIS-direktivet var till stor del ett analogt svar på ett digitalt problem.”

Trots de tuffare rapporteringskraven i NIS-direktivet och det kontinuerligt ökande säkerhetshotet, visar MSB:s årsrapport för IT-incidentrapportering på en sammantagen minskning av antal inrapporterade incidenter de senaste tre åren[18]. Den förhöjda hotbilden översätts inte ovillkorligen i genomförda incidenter, men i ett flertal rapporter över hotlandskapet konstateras en ökning i både antal incidenter, och dess påverkan på verksamheter[3],[21],[28]. Av MSB:s incidentstatistik att döma finns det därmed anledning att tro att det finns ett stort mörkertal av cyberbrott, vilket myndigheten själva medger. Trots kraven så rapporteras alltså inte incidenter in, vilket är problematiskt eftersom information om incidenter hjälper till att skapa en större förståelse för hotbilden och bidrar till att stärka samarbetet runt det förebyggande arbetet.

Tuffare krav och ökad tydlighet

För att komma till rätta med denna problematik, harmonisera arbetet, stärka den inre marknaden och framtidssäkra medlemsländernas digitala motståndskraft beslutades om införandet av NIS2-direktivet i slutet av 2022 vilket skall vara implementerat i nationell lagstiftning senast 17 oktober 2024[7]. En väl insatt specialist menar att NIS2 kommer uppfattas vara mer konkret och praktiskt betonat och kommer dessutom närmare verksamheten än NIS. Tanken är att mer insatser skall läggas på rutiner och förvaltning än tidigare för att bibehålla efterlevnaden av ramverket. Ackrediteringsinstitutet DNV väljer att använda uttrycket ”NIS2 är NIS på steroider”[1].

Sverige har tillsatt en statlig offentlig utredning som ska ta ställning till hur direktivet ska regleras i svensk lag[23]. Nedan visas en enkel tidslinje över implementeringen.

Värt att nämna är att NIS2-direktivet följer samma tidslinje och skall implementeras tillsammans med det så kallade CER-direktivet (direktiv för stärkt motståndskraft i samhällsviktig verksamhet). CER-direktivet är inte fokus för denna rapport, men för de verksamheter som berörs finns anledning att arbeta med de båda direktiven parallellt. Regleringen av CER bedöms i samma pågående utredning.

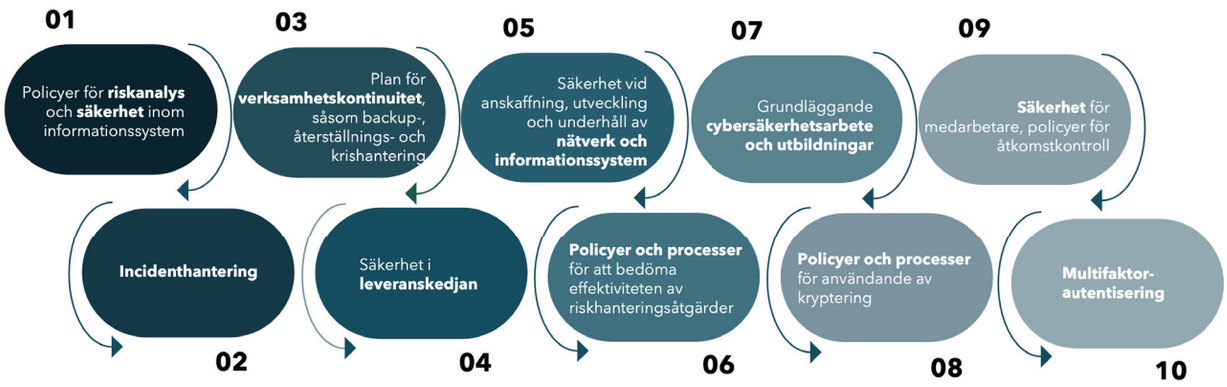
De största skillnaderna

Genom tydligare krav och ansvarsutkrävande är förhoppningen att NIS2 skall bidra till att överkomma problemen med det tidigare direktivet. Några av de största och viktigaste skillnaderna i NIS2-direktivet innefattar[7]:

- **Utvidgat tillämpningsområde** – Fler sektorer omfattas, och en storleksregel införs för att förenkla och harmonisera tillämpningen mellan medlemsländerna
- **Ökade säkerhetskrav och krav på incidenthantering** – Direktivet fastställer en minimistandard för säkerhetsåtgärder och incidenthantering för att höja den gemensamma säkerhetsnivån. Medlemsländerna kan besluta om tillägg eller skärpta krav, men direktivet utgör den grundnivå som skall implementeras.
- **Införande av sanktioner** – För de verksamheter som brister i sin efterlevnad kan sanktioner utdelas på upp till 10 miljoner EUR eller 2 procent av den globala årsomsättningen.
- **Säkerhetskrav i leverantörskedjan** – För att hantera den tilltagande tredjepartsrisken utökas säkerhetskraven till att även omfatta verksamhetens leverantörsled.
- **Ökade krav på ledningen** – De styrande organen i verksamheterna (som bolagsstyrelse eller kommunstyrelse) är ansvariga för att godkänna säkerhetsåtgärderna och övervaka dess implementering och kan även hållas ansvariga vid bristande efterlevnad. Ledningen behöver genomgå utbildning för att kunna identifiera risker och bedöma riskhanteringsåtgärder och dess påverkan på de tjänster som verksamheten levererar.

Nya säkerhetsåtgärder

Som en del av arbetet med att implementera NIS2-direktivet behöver verksamheter etablera policyer och processer som innefattar allt ifrån riskanalys, kontinuitets- och incidenthantering till utbildningar och åtkomstkontroll. Därtill så är säkerhet i leverantörsledet ett nytt område där verksamheten själv ansvarar över att säkerställa att ens leverantörer uppfyller kraven. Nedan redovisas de 10 säkerhets-åtgärder som specificeras i NIS2-direktivet och som gäller som minimikrav[7].



3.2 Fler sektorer och verksamheter omfattas

Utöver de sektorer som sedan tidigare omfattas av NIS, tillkommer nu fler sektorer under NIS2-direktivet[4]. En av de stora utmaningarna med NIS var att verksamheterna själva skulle uppskatta om de omfattades och anmäla det till en tillsynsmyndighet, vilket medförde stora skillnader i hur direktivet tillämpades mellan medlemsländerna. För att förenkla och harmonisera arbetet med att identifiera samhällskritiska verksamheter under NIS2 införs en storleksregel. Grundregeln är att medelstora och stora bolag som är verksamma i de utpekade sektorerna omfattas av NIS2[7]. Därtill kan varje land besluta om inkludering av mindre bolag som bedriver verksamhet som är av stor vikt för samhället, ekonomin eller för de sektorer som omfattas av direktivet.

Upp till 40 gånger fler verksamheter omfattas

Uppskattningsvis rör det sig om cirka 150 000 organisationer och verksamheter som kommer att omfattas av NIS2 i Europa, och motsvarande siffra för Sverige bedöms landa cirka 10 000 verksamheter, men kan omfatta så många som 20 000 svenska verksamheter[30,31]

Anledningen till att upp emot 40 gånger fler verksamheter kommer att omfattas av NIS2 jämfört med dagens NIS är dels att fler sektorer tillkommer och dessutom omfattas fler verksamheter inom de befintliga sektorerna. Vidare så berörs leverantörsledet hos dessa verksamheter vilket kraftigt bidrar till det ökade antalet.

500	x7–40	3 500–20 000
Berörda verksamheter av NIS-lagen i Sverige	Uppskattad andel fler verksamheter i Sverige som berörs av NIS2	Uppskattat antal verksamheter i Sverige som berörs av NIS2[30,31]

Fler sektorer och en ny indelning

Sektorerna klassificeras i NIS2-direktivet som väsentliga eller viktiga entiteter, varav de väsentliga möter tuffare krav, främst i form av högre bötesbelopp samt proaktiv tillsyn[7]. Den statliga offentliga utredningen ska ta ställning till vilka myndigheter som ska anförtros tillsynsansvaret gentemot de nytillkomna sektorerna[23].

Väsentlig entitet	Viktig entitet
Energi – Tillsynsmyndighet: Energimyndigheten	**Postverksamhet**
Transport – Tillsynsmyndighet: Transportstyrelsen	**Avfallshantering**
Digital infrastruktur – Tillsynsmyndighet: Post- och telestyrelsen	**Digitala leverantörer** · Internetbaserade marknadsplatser · Sökmotorer · Sociala nätverkstjänster
Bankverksamhet – Tillsynsmyndighet: Finansinspektionen	**Produktion och distribution av livsmedel**
Finansmarknadsinfrastruktur Tillsynsmyndighet: Finansinspektionen	**Produktion och distribution av kemikalier**
Hälso- och sjukvård – Tillsynsmyndighet: Inspektionen för vård och omsorg	**Tillverkningsindustrin** · Medicinska apparater · Datorer, elektroniska och optiska produkter · Elektrisk utrustning · Maskiner · Motorfordon, släpvagnar och semitrailers · Annan transportutrustning
Leverans och distribution av dricksvatten Tillsynsmyndighet: Livsmedelsverket	
Offentlig förvaltning · Statliga myndigheter · Regioner · (Kommuner under utredning)	
Avloppshantering	
Rymdverksamhet	

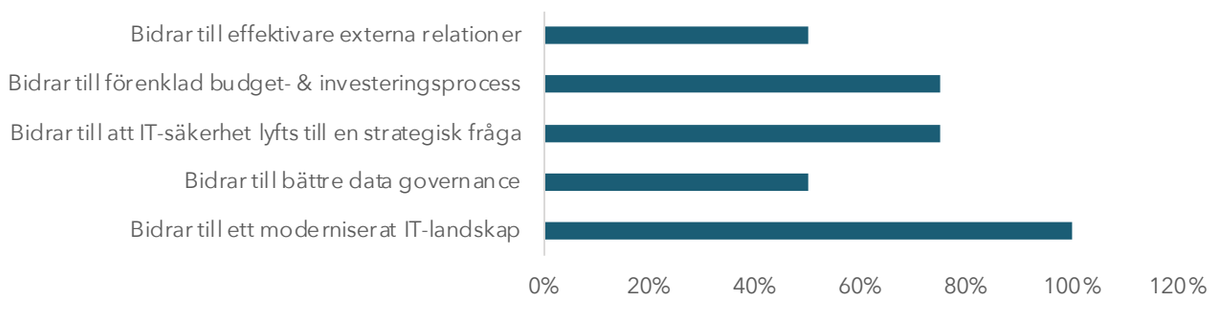
Trots storleksregeln och arbetet med att förtydliga bestämmelserna finns det fortfarande frågetecken när det kommer till omfattningen av svenska verksamheter. Exempelvis så är det inte helt tydligt hur sektorn offentlig förvaltning skall tolkas i en svensk kontext, där regeringens kommittédirektiv fastställer att statliga myndigheter och regioner omfattas, men där den statliga offentliga utredningen skall ta ställning till huruvida den kommunala verksamheten ska omfattas i sin helhet eller inte[23].

Det generella rådet för de verksamheter som är osäkra på huruvida de omfattas eller inte är att utgå ifrån att så är fallet, särskilt vad gäller medelstora och stora verksamheter inom de utpekade sektorerna. Eftersom direktivet väntas beröra uppemot 20 000 svenska verksamheter kommer NIS2 att vara relevant att ha koll på för samtliga svenska verksamheter, oavsett om de träffas direkt eller inte. Dels kommer det att vara en förutsättning för att verka i leverantörsrelationer med verksamheter i de utpekade sektorerna, dels är det troligt att cybersäkerhet och NIS2-krav kommer att dyka upp i avtal och affärsrelationer i allt högre utsträckning. Vidare är den förhöjda hotbilden viktig för samtliga verksamheter att vara medvetna om och hantera då cyberbrottslingar ständigt söker och nyttjar nya sårbarheter. Cybersäkerhetsmognaden är generellt sett för låg och det finns ett stort behov av att höja garden – oavsett om man måste göra det genom direktivet eller inte. En högre cybersäkerhetsförmåga innebär även att verksamheten minskar risken att drabbas av kostsamma incidenter och säkrar värdet av den egna digitaliseringen. NIS2 bör ses som ett verktyg och möjliggörare för att uppnå detta.

3.3 Regulatoriska krav bidrar till en säker digitalisering

Regulatoriska ramverk bidrar till en säkrare digitalisering genom att påbjuda en högre gemensam standard för säkerhet som skapar förutsättningar för en rad positiva effekter. Genom att etablera en säker grund och minska riskerna för att verksamheten utsätts för skadliga och kostsamma incidenter kan ramverken bidra till både positiva interna och externa effekter som underlättar i digitaliseringen.

Andel (%) **respondenter som anger positiva effekter av regulatoriska ramverk**



Att hantera cybersäkerhet har blivit en grundförutsättning för att kunna existera som verksamhet på den digitala marknaden och NIS2 kan tjäna som ett verktyg för verksamheter i det säkerhetshöjande arbetet. Att säkerställa en säkrare gemensam grund kommer dessutom att bygga tillit och vara en förutsättning för effektivt samarbete mellan olika parter. Direktivet bidrar även till att höja cybersäkerhet till en strategisk bolagsfråga och förordnar en övergripande kompetenshöjning inom verksamheten, vilket är värdefullt då det råder en generell brist på cybersäkerhetskompetens i samhället just nu. Genom att etablera en gemensam standard för cybersäkerhet inom unionen stärks även den inre marknaden och bidrar till ett ökat skydd för individer, verksamheter och nationer.

4. Ett bransch-perspektiv på NIS2

NIS2 omfattar ett stort antal verksamheter inom både privat och offentlig sektor. De krav och de säkerhetsåtgärder som specificeras är utformade för att vara enklare att tolka och tillämpa än den tidigare versionen av direktivet för att säkerställa en harmonisering mellan olika länder, verksamheter och sektorer. Olika sektorer har dock olika vana och erfarenhet av att arbeta med regulatoriska krav och skillnaden i mognadsgrad och förutsättningar gör det intressant att jämföra dem.

I detta kapitel undersöks NIS2 ur fyra aktuella sektorers perspektiv: bank och finans, kritisk infrastruktur, regioner och kommuner. Skillnader i förutsättningar, utmaningar och mognadsgrad presenteras och efterföljs av branschspecifika rekommendationer för att komma i gång med arbetet. Grunden till branschperspektiven utgörs till stor del av intervjuer med respondenter från respektive bransch eller sektor.

Varför är följande samhällssektorer intressanta?

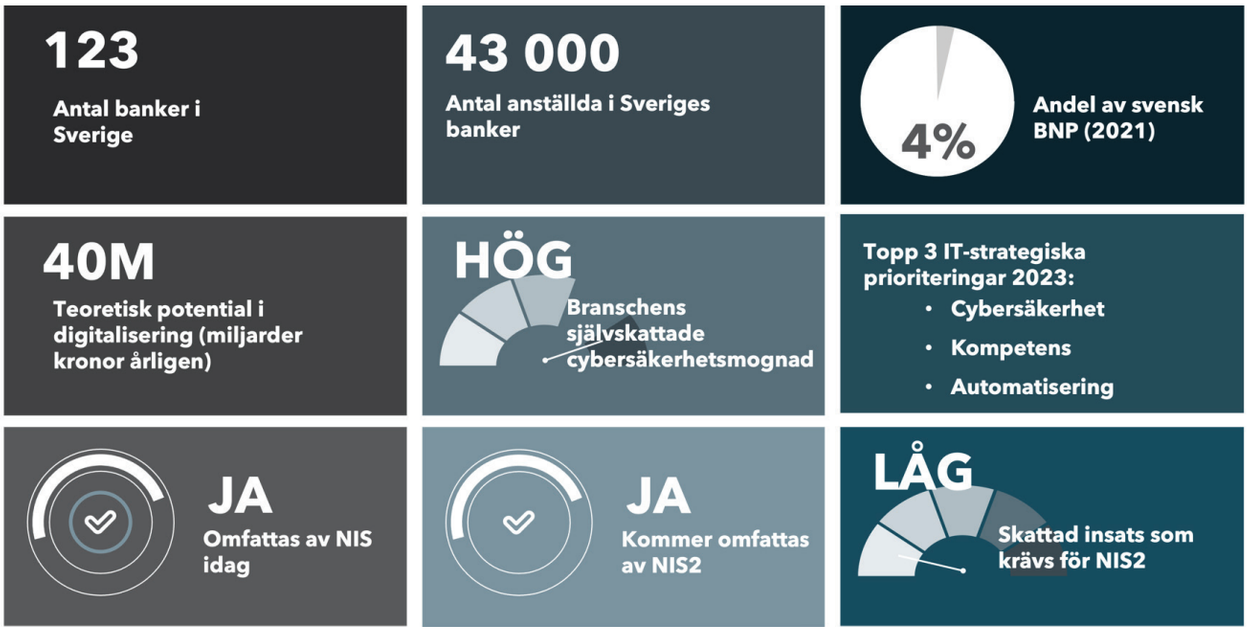
Bank och finans – En sektor som har en stor vana vid att hantera regulatoriska ramverk och tillsyn. Aktörer inom bank- och finanssektorn har ett välutvecklat riskhanteringsperspektiv och frågan har ett högt fokus hos ledningen. Detta fokus är delvis ett resultat av de allvarliga konsekvenser och höga sanktionsavgifter som verksamheter som brister i sin efterlevnad möter. Med introduktionen av nya regulatoriska ramverk skall detta riskperspektiv breddas till att även innefatta cybersäkerhet i högre utsträckning.

Samhällskritisk infrastruktur – Här ligger fokus på aktörer som hanterar anläggningar och strukturer som är kritiska för ett fungerande samhälle. Dessa aktörer har till stor del ett utpräglat säkerhets-perspektiv, men där arbetet med cybersäkerhet ofta har ett mer tekniskt än strategiskt fokus. Den förändrade geopolitiska hotbilden gör samhällskritisk infrastruktur till ett prioriterat mål för cyberhot och därmed en prioriterad sektor att öka robustheten inom.

Region – En stor och omfattande sektor som har en vana vid att arbeta med bland annat lagar och förordningar som rör patientsäkerhet, men där kunskap och förmåga runt cybersäkerhet är mer begränsad. Hälso- och sjukvård innefattas av den rådande NIS-lagen, men där regioner nu kommer att omfattas i sin helhet i och med att offentlig förvaltning introduceras som ny sektor under NIS2. Den åldrande befolkningen medför att digitalisering och därmed även cybersäkerhet blir en kritisk fråga att hantera för regionerna.

Kommun – Det är ännu oklart om kommuner kommer att omfattas i sin helhet inom NIS2, eller endast de delar av den kommunala verksamheten som berör samhällskritisk infrastruktur. Detta en sektor med en generellt sett låg kunskap och förmåga kring att hantera cybersäkerhet så det finns ett stort behov av att höja säkerhetsnivån i verksamheten. Utmanande för kommunerna är det faktum att det råder stora skillnader i storlek och förutsättningar dem emellan och det kommer att krävas insatser och resurser för att uppnå en högre cybersäkerhet.

4.1 Bank och finans



Tabellreferenser: 16, 24, 25

4.1.1 NIS2 ur ett bank- och finansperspektiv

Bank- och finanssektorn är både historiskt sett, och i dagsläget en av de mest utsatta sektorerna i samhället när det kommer till cyberhot och incidenter. Det är av kritisk betydelse att samhället upprätthåller ett högt förtroende för den finansiella sektorn, och det är även den sektor där incidenter har störst negativ påverkan på just rykte och förtroende[3]. Därtill är den finansiella marknaden och verksamheterna nära sammankopplade vilket medför att problem snabbt kan spridas, samtidigt som den finansiella sektorn har starka beroenden även mellan andra sektorer[11]. Att kunna genomföra transaktioner och betalningar är avgörande för ett fungerande samhälle och incidenter och avbrott får snabbt allvarliga konsekvenser.

Givet detta är regulatoriska krav inget nytt för aktörer inom denna sektor att hantera. Kostnaderna för regelefterlevnad bedöms ha ökat kraftigt de senaste åren, samtidigt som vi sett ett flertal exempel på hur höga kostnaderna kan bli för de verksamheter som brister i sin efterlevnad i form av utdelade böter och sanktionsavgifter. Det omfattande regulatoriska landskapet är en återspegling av de skyddsvärden som denna sektor bedöms inneha.

Den befintliga NIS-lagen gäller även för denna sektor som således redan en vana kring att arbeta med informationssäkerhet. Det gör bank och finans till en intressant sektor att ta rygg på vid införandet av NIS2 då branschen och tillsynsmyndigheten har en väl beprövad och fungerande relation. Andra sektorer kan därmed titta på grundläggande principer och goda exempel från bank och finans och dra lärdom av dem för det egna implementeringsarbetet.

”Jag ser de regulatoriska kraven som något positivt, och jag hör bara positivt från andra. Det ökar kvalitén i leveransen.”

Vad beträffar NIS2 så kan det ses som ytterligare ett direktiv av flera som skall implementeras inom kort, samtidigt som efterlevnaden av befintliga ramverk ska bibehållas. Utöver att förhålla sig till NIS2 så träffas de även av den så kallade DORA-förordningen (förordningen om digital motståndskraft). Båda regleringarna följer i stort sett samma tidslinje och det finns en del överlapp mellan ramverken, men där DORA förväntas överskugga de mer generella bestämmelserna i NIS2. DORA-förordningen kan därmed ses som ett skarpare och mer specialiserat ramverk särskilt inriktat mot de utmaningar som verksamheter inom bank och finans står inför. En första bedömning är att NIS2-implementationen inte kommer upplevs som alltför krävande då mycket redan finns på plats, men som kräver ett strukturerat tillvägagångssätt.

4.1.2 Utmaningar och hot

Den största utmaningen är just den omfattande hotbilden. Bank och finans är den sektor som utsätts för flest attacker och intrångsförsök, där incidenter har störst effekt på varumärke och förtroende, men även de dyraste incidenterna. Det är dessutom den sektor som lider mest av interna misstag, det vill säga att den interna hotbilden är förhöjd. De vanligaste intrångsförsöken sker genom phishing som blir alltmer sofistikerat med hjälp av ny teknik, eller hackning med stulna inloggningsuppgifter. Det transformerande hotlandskapet drivet av teknikutvecklingen medför att det är det kritiskt att sektorn besitter aktuell kunskap, har en anpassad säkerhetskultur och en uppdaterad riskhanteringsprocess.

En återkommande utmaning som sektorn har tillsammans med framför allt kritisk infrastruktursektorn är att aggregera de olika riskanalyserna för att uppnå en samlad och effektiv incident- och kontinuitetshantering. Detta kan uppnås först när verksamheten har insikten om behovet och tar ansvar över att driva detta arbete.

Ytterligare en utmaning är leverantörsstyrningen som kommer in via både NIS2 och DORA. Det finns en risk att leverantörer, oftast mindre, inte inser ansvaret och insatserna som krävs för att uppnå efterlevnad av regelverken. Det kommer vara viktigt att se över avtal och säkerställa att leverantörerna kan bygga och utveckla den nödvändiga förmågan för att leva upp till de högt ställda krav som denna sektor har.

Samverkan mellan olika aktörer inom bank- och finanssektorn är väl utvecklad, men trots det kommer NIS2 kräva nya former av samverkan med andra externa aktörer som även de berörs av direktivet samt andra tillsynsmyndigheter. Detta hänger samman med att övriga samhället är starkt avhängt ett robust finansiellt system för att fungera och det finns många beroenden och sammankopplingar mellan olika aktörer och tjänster. Behov av ny typ av samverkan kommer alltså att vara nödvändigt.

4.1.3 Mognadsgrad

Att förhålla sig till tuffa regulatoriska krav och lagar är inget nytt för finansiella aktörer. En ökad mognadsgrad har byggts upp genom etablerade rutiner, processer och praxis i den egna organisationen, men även samverkansforum och nätverk som är av särskild betydelse givet den nära sammankopplingen av finansiella aktörer. Därtill finns en väl etablerad kultur och medvetenhet kring säkerhet hos både kunder och inom den egna verksamheten, samt en god anmälnings- och rapporteringskutym i branschen. Formella tillstånd, lagar och förordningar har uppdaterats med cybersäkerhetsreglementen. Tillsynsmyndigheter, dess inspektioner och sanktionsavgifter är etablerade i branschen. Detta gör också att insikt och förmåga kring risk och säkerhet hos den högsta ledningen är generellt högre inom denna sektor, vilket underlättar för en säkerhetskultur inom verksamheten och medför att nödvändiga investeringar och aktiviteter kan drivas igenom enklare.

”Vi som bransch har kommit så långt att säkerhet nu är en naturlig del av vårt dna”.

Bank- och finanssektorn är starkt digitaliserad och idag är nästan alla tjänster som tillhandahålls digitala. Tillsammans med ett starkt säkerhetsfokus medför det att sektorn som utgångspunkt har en högre digital motståndskraft vilket skyddar kärnverksamheten och ger en högre förmåga att tillvarata digitaliseringens möjligheter. En vana och rutin kring regulatoriska krav gör det också snabbare och enklare att hantera nya krav som kommer vilket är en fördel.

Andra branscher och sektorer ser bank- och finanssektorn tillsammans med tillsynsmyndigheten Finansinspektionen som ledande i att bygga upp en holistisk cybersäkerhetsförmåga och säkerhetskultur, både i sina organisationer men även hos sina kunder och som bransch. Det som lyfts fram som starka förmågor i bank- och finanssektorn är exempelvis:

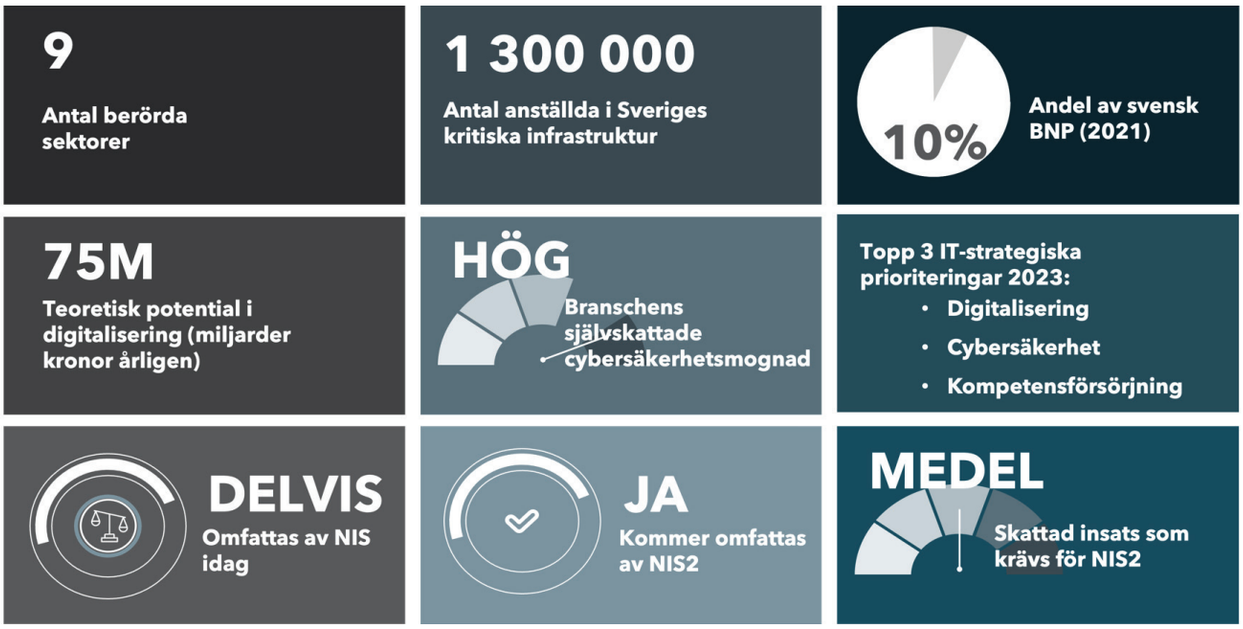
Anmärkningsvärt är att branschen som helhet klarat av att bygga upp en mognad kring cybersäkerhet, trots att det generellt finns en teknisk skuld i branschen med många applikationer och infrastruktur på gammal teknik (till exempel COBOL och stordatormiljöer). En risk bank- och finanssektorn har lyckats hantera.

Bibehållen förmåga och efterlevnad över tid i organisationen	**Ledningens engagemang**	**Rapporterings- och uppföljningskultur**
Samverkan inom branschen	**Tillsyns-, efterlevnads- och sanktionssystem**	**Proaktivitet och förmåga att reagera snabbt vid incident**

4.1.4 Call to action

1	**Starta nu!** Det kommer vara enklare för aktörer inom bank- och finanssektorn att implementera NIS2 på grund av erfarenheter av tidigare lagar och förordningar. Därför är det bara att börja. Nyttja befintlig best practice från verksamheten för implementering av NIS2.
2	**Gemensam koordinering** Studera de aktuella och närliggande ramverken, såsom DORA-förordningen och CER-direktivet, som också skall implementeras och genomför en analys och etablera en plan i gemensam process.
3	**Leverantörslandskap** Analysera leverantörslandskapet tidigt för att fånga de leverantörer som kan behöva extra stöd för att bygga förmåga runt de nya kraven. Engagera även befintliga leverantörer för att etablera samverkansformer runt riskhantering och säkerhetsåtgärder.

4.2 Samhällskritisk infrastruktur



Tabellreferenser: 16, 19, 24, 26

4.2.1 NIS2 ur ett kritiskt infrastrukturperspektiv

En delmängd av de verksamheter som MSB definierar som samhällsviktiga utgör kritisk infrastruktur och kan godtyckligt uppskattas till nio verksamhetsområden (se tabell nedan). Dessa verksamheter kan utgöras av både offentliga verksamheter och privata aktörer. Alla sektorer som innefattas av NIS2-direktivet kan antas utgöra samhällskritisk infrastruktur på olika sätt, men sammanställningen i detta delkapitel syftar till att lyfta perspektivet från aktörer som hanterar anläggningar och strukturer som är kritiska för ett fungerande samhälle. Detta innefattar:

Transport	Finansmarknadsinfrastruktur	Energiförsörjning
Dricksvatten	Avloppshantering	Avfallshantering
Digital infrastruktur	Rymd (markbaserad infrastruktur)	Produktion och distribution av livsmedel

Samhällskritisk infrastruktur är i hög grad beroende av digitala system och teknologi vilket introducerar en del potentiella sårbarheter som kan utnyttjas. Infrastrukturen är ofta mycket komplex, med många olika system och komponenter som samverkar. Denna komplexitet skapar utmaningar när det gäller att säkerställa att varje del av infrastrukturen är säker och skyddad och således kan en sårbarhet i en del av infrastrukturen potentiellt påverka hela systemet. Beroende på vilken typ av infrastruktur som påverkas och omfattas kan konsekvenserna av en cyberattack vara långtgående och påverka både enskilda medborgare och samhället i stort.

Idag finns i huvudsak tre regulatoriska krav och ramverk som omfattar samhällskritisk infrastruktur som syftar till att säkerställa dess driftsäkerhet och integritet. Dessa innefattar NIS-lagen, ISO 27001 och IEC 62443 (Industrial Automation and Control Systems Security).

”De senaste ramverken har faktiskt varit en tillgång för vår sektor som helhet, men även för vår egen verksamhet”.

4.2.2 Utmaningar och hot

Aktörer inom samhällskritisk infrastruktur använder ofta system med digital teknik för att hantera fysiska processer, det vill säga operativ teknik (OT). Det senaste året har hotet mot kritisk infrastruktur och mot OT ökat och förväntas öka ytterligare[3]. Bedömningen är att framför allt statligt backade aktörer just nu har ett ökat intresse för att bedriva underrättelseverksamhet mot dessa mål för att bygga förmåga för att kunna utföra attacker i framtiden[3]. Generellt har verksamheter kommit mycket längre med IT-säkerhet än OT-säkerhet och OT-system har många sårbarheter i form av gamla enheter som körs på icke uppdaterad mjukvara, samt strukturella säkerhetsrisker som uppstått genom en osäker digitalisering. I takt med att IT och OT integreras för att möjliggöra bland annat automation och realtidsanalyser så skapas en risk för verksamheten att drabbas av attacker och intrång som sker via de sämre säkrade OT-enheterna. Det är viktigt att förstå och hantera denna risk som en del av arbetet med att säkra nätverk och informationssystem inom verksamheten.

En potentiell utmaning som en del aktörer inom samhällskritisk infrastruktur kan komma att uppleva, är att det kan krävas en omfattande strategiomläggning runt befintlig outsourcing av IT. Där nya krav på ansvarsfördelning, åtagande och riskhantering måste kompletteras med NIS2-specifika krav till den nuvarande relationen. Även övriga delar av leverantörsansvaret, som inte är kopplade till endast outsourcing av IT, utan all kritisk försörjning i leverantörsledet kommer vara mycket krävande för verksamheten att adressera och bibehålla en efterlevnad inom. Då denna sektor är van vid att definiera och riskhantera olika attackytor kommer utmaningen ligga i den samlade riskhanteringen, dokumenteringen och rapporteringen.

Som tidigare nämnts kan inte efterlevnad av NIS2 uppnås genom enbart tekniska cybersäkerhets-initiativ, utan säkerhetsarbetet behöver genomsyra hela verksamheten och hanteras mycket mer strategiskt än det ofta görs idag. Därför är det viktigt att ledningen aktiveras och engagerar sig i högre utsträckning i detta arbete.

”Cybersäkerhet har kommit att bli en bolagsfråga. Enligt min mening kommer det vara avgörande hur väl man lyckas lyfta upp cybersäkerheten som en digital affärsrisk på ledningsnivå. Det saknas en best practice för hur man bäst jobbar med detta som en strategisk ledningsfråga.”

Den generella säkerhetskulturen är god bland medarbetare inom samhällskritisk infrastruktur, så det finns en bra grund att bygga vidare på. Med det sagt kommer det att krävas utbildning av personal för att höja cybersäkerhetskompetensen ytterligare vilket ofta kräver tid och resurser.

4.2.3 Mognadsgrad

Offentliga verksamheter och privata aktörer inom samhällskritisk infrastruktur är vana vid att tillämpa säkerhetsskyddslagar och förordningar som både gäller fysisk, data-, informations- och IT-säkerhet. Det är inte ovanligt med tillsyn tillsammans med till exempel säkerhetstjänster. Det finns också en mognad och förmåga kring att definiera olika typer av attackytor i verksamheten och riskhantera dessa. Däremot finns det delar inom NIS2 som kommer kräva en ny förmåga runt cybersäkerhet i framför allt verksamheten som ofta inte finns idag. Exempel på detta är incident- och kontinuitetshantering, leverantörsansvar samt ledningens styrning och uppföljning.

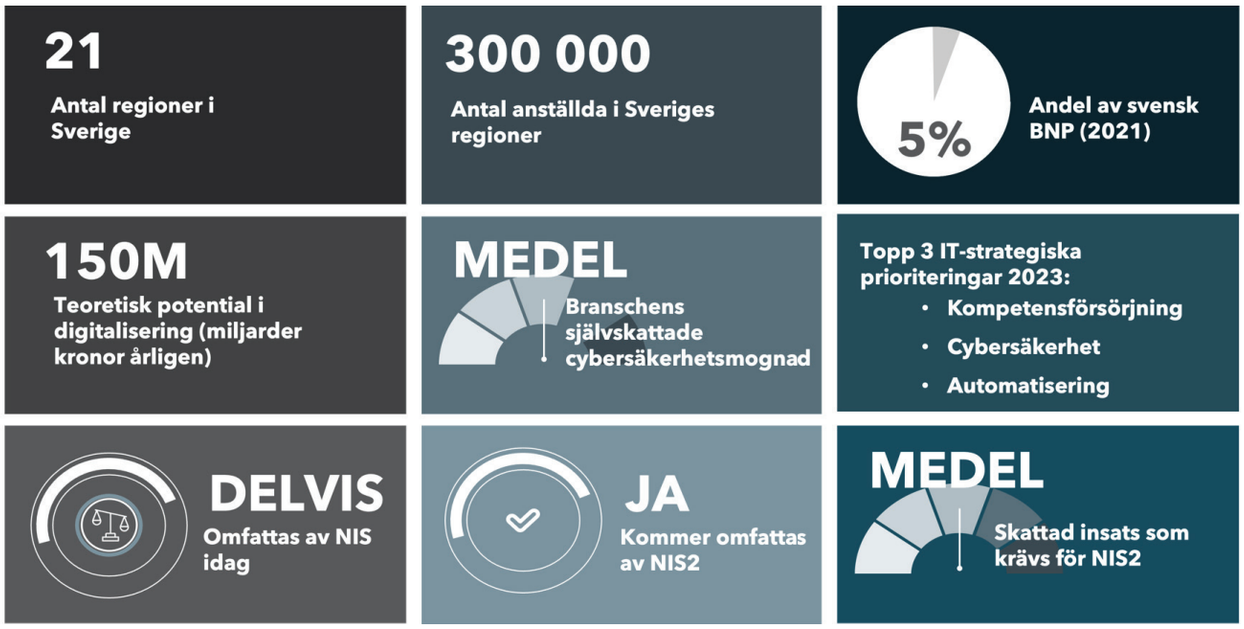
Att tillhandahålla säkra allmännyttiga tjänster till samhället och samtidigt uppfylla ständigt föränderliga regleringskrav är en påfrestning. Sektorns natur, med komplexa system och komponenter, bidrar till en långsam moderniseringsprocess. Denna tekniska skuld ökar exponeringen för cyberhot.

Den generella uppfattningen bland aktörer inom samhällskritisk infrastruktur är att regulatoriska ramverk, såsom NIS2, ökar digitaliseringstakten. Framför allt på grund av det som nämns ovan om nödvändig teknisk modernisering, men även genom att det bygger ett starkare förtroende till partners och leverantörer som har förmåga och god efterlevnad av ramverken. De regulatoriska ramverken uppfattas därför som plattformar för säker digitalisering inom denna sektor.

4.2.4 Call to action

1	**Starta nu!** Aktörer inom samhällskritisk infrastruktur med sina komplexa miljöer kommer behöva mycket tid för att implementera NIS2. Om externt stöd krävs är det ofta en fråga om säkerhetsklassad personal, vilket det råder stor brist på. Därmed finns det ingen tid att förlora.
2	**Verksamheten** Aktivera verksamheten omgående för att få en lägesbild om behov och möjliga gap som behöver hanteras för att uppnå efterlevnad. Börja även kartlägga och utvärdera läget inom leverantörslandskapet omgående.
3	**Ledningen** Det finns ett behov av ett snabbt strategiskt inriktningsbeslut tillsammans med fördelat ansvar och mandat för att få den tidiga starten som kommer vara viktig för denna sektor. Därtill behöver ledningen följa upp det kontinuerliga arbetet för att säkerställa ett bibehållet fokus och prioritering i verksamheten.

4.3 Region



Tabellreferenser: 16, 19, 24, 26

4.3.1 NIS2 ur ett regionperspektiv

De 21 regionerna i Sverige sysselsätter över 300 000 anställda och motsvarar mer än 5 procent av Sveriges totala BNP 2021 vilket gör regionerna till en viktig samhällsaktör. Den befintliga NIS-lagen innefattar hälso- och sjukvård, men offentlig förvaltning är en ny sektor inom NIS2 där statliga myndigheter och regioner som helhet kommer att innefattas[23]. Därmed finns redan en viss vana vid att arbeta med lagar, förordningar och regulatoriska ramverk, men där regionerna kommer behöva göra en insats för att sätta sig in i och uppfylla kraven för NIS2.

År 2030 kommer Sveriges befolkning som är över 80 år att ha ökat med 50 procent[33]. Det är den enskilt största utmaningen för både regioner och kommuner. Delvis för att denna förflyttning av befolkningsmix kommer öka behovet av välfärd och sjukvård, men det är även en utmaning ur ett ekonomiskt perspektiv för att bibehålla välfärdsnivån i hela samhället. Utmaningen är av den dignitet att varken region eller kommun kommer att klara av detta genom nyrekrytering, så både region och kommun ser därför säker digitalisering som en viktig komponent för att lösa detta. Givet detta kan NIS2-direktivet utgöra ett verktyg och en plattform att nyttja för att klara den gemensamma säkra digitaliseringen. Dock är NIS2-direktivet relativt okänt som begrepp just nu i verksamheterna både ur ett region- och kommunperspektiv.

”NIS2-direktivet är ett tämligen okänt begrepp ännu i offentlig verksamhet. På en fråga skulle kanske 10% av verksamhetsledningar i regioner och kommuner vara insatta i frågan, vilket kan jämföras med att samma nivå gällande GDPR är nästintill 100%.”

4.3.2 Utmaningar och hot

Det faktum att offentlig förvaltning i sin helhet inkluderats i NIS2-direktivet är ett resultat av den ökade hotbilden mot denna sektor. En analys av hotlandskapet från föregående år visar att offentlig sektor är en av de mest utsatta sektorerna när det kommer till antal genomförda attacker och liksom för bank- och finanssektorn får det stora konsekvenser för rykte och förtroende[3]. Främst handlar det om incidenter kopplade till stöld av personuppgifter och data, eller störningar och avbrott i tjänster vilket bidrar till att undergräva förtroendet för våra samhällsinstitutioner. Att aktörer inom offentlig sektor nu höjer sin försvarsförmåga är därmed av yttersta vikt för vår samhällsutveckling.

En utmaning som lyfts upp från regionerna är att diskussionen runt implementeringen av NIS2 inte får bli för kortsiktig och minimalistisk och kännetecknas av stress, kortsiktiga beslut eller för stort fokus på den mest lättvindiga vägen till teknisk efterlevnad. Den allmänna uppfattningen är dock att NIS2, om det hanteras på ett bra sätt, kan stödja verksamheternas fortsatta digitalisering på ett positivt sätt.

Det ligger även en utmaning i att undvika att NIS2-implementeringen hanteras i olika och separerade stuprör, där teknisk IT-säkerhet hanteras på en nivå, den juridiska aspekten på en annan och verksamheten gör åtgärder för sig. Då tappas lätt den nödvändiga samlade riskhanteringen som är central i NIS2. Det kommer då även bli svårt att få en bred insikt om cybersäkerhetskulturen i organisationen och högst troligt kommer den gemensamma incident- och kontinuitetshanteringen bli mycket svår att få till. Efterlevnaden riskerar då att bli eftersatt. Även om regionerna har en god mognad runt strukturer för utvärdering, uppföljning och förbättring runt tekniska säkerhetsåtgärder anser sig sektorn inte ha något befintligt ledningssystem (process samt IT-stöd) som kommer uppfylla de behov och krav som NIS2 kommer innebära för regionerna.

Arbetet för att implementera NIS2 kommer att driva kostnader och kräva investeringar, vilka till stor del inte är budgeterade ännu. Den egna bedömningen är att det finns en förmåga för att skapa en inledande förståelse för vad NIS2 kommer kräva av verksamheten, en så kallad GAP-analys, men där det kommer krävas extern hjälp i själva implementeringen. För en

sektor med lägre grundkunskap om NIS2 är att det extra viktigt att komma i gång snabbt. Nödvändiga ekonomiska beslut behöver fattas så snart som möjligt för att inte tappa alltför mycket värdefull tid i arbetet.

”Verksamhetschefer behöver få en mer långsiktig tilldelning av resurser för att över tid klara av att bygga upp en hållbar förmåga och efterlevnad i sin egen organisation. Detta gäller både för den viktiga digitaliseringen men även för cybersäkerhet.”

4.3.3 Mognadsgrad

Regioner uppfattas i allmänhet vara mer IT-säkerhetsmogna än kommuner men mindre mogna än myndigheter. Anledningen till att regioner bedöms mer mogna än kommuner är till att börja med att en förhållandevis stor del av den regionala verksamheten är hälso- och sjukvårdsrelaterad och som omfattas av många lagar, förordningar och regulatoriska ramverk. Därtill är regioner oftast större organisationer i sin natur och har på så sätt större enheter med tilldelat ansvar, fler medarbetare och är därmed inte lika sårbara för personberoenden. Dessa två anledningar underlättar att både bygga upp en cybersäkerhetförmåga och sedan underhålla den.

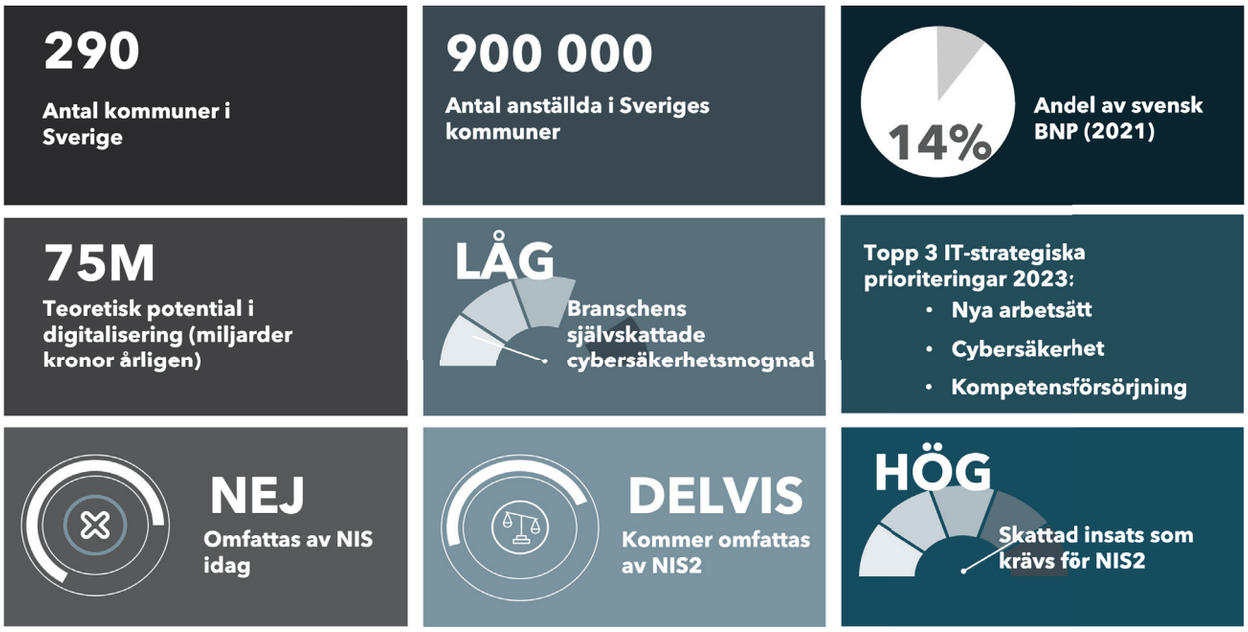
De redan implementerade ramverken som finns i regionerna har bidragit till en förmåga att ta till sig nya ramverk, analysera dessa och skapa insikt om vad som behöver göras. Dock kommer NIS2 att kräva ett cybersäkerhets-fokus om kommer vara nytt för regionerna. Regionerna har idag kommit långt när det gäller informationsklassning och att arbeta strukturerat med informationssäkerhetsrisker. Till skillnad från kommunerna har regionerna i högre utsträckning en god vana kring att säkerhetsställa informationssä-kerhet på ett strukturerat sätt vid exempelvis upphandlingar.

Det finns flera välutvecklade forum och nätverk för regioner (så som SLIT, e-hälsomyndigheten, SKR, Inera) för att utbyta best practice och goda exempel. En lärdom från tidigare implementeringar av ramverk är att SKR har en avgörande roll i att tidigt förtydliga tolkningar och ta fram relevanta praxis för att det skall bli en effektiv och gemensam implementering och undvika egna tolkningar och dubbelarbete.

4.3.4 Call to action

1	**Engagera SKR** Engagera nätverken med regionalt fokus inom SKR för att få nödvändiga förtydliganden och praxis anpassade för regioner. Syftet är att undvika egna tolkningar och maximera synergieffekter.
2	**Regionledning** Aktivera regionledningen för att tidigt ta inriktningsbeslut samt dela ut ansvar och mandat i verksamheten. Arbetet med att höja cybersäkerheten kommer att kräva resurser och möjligen extern hjälp vilket det behöver budgeteras för.
3	**Utbildning** Det saknas en bred insikt om NIS2-direktivet och vad det innebär ute i verksamheterna. Påbörja arbetet med utbildning och kompetensutveckling inom cybersäkerhet snabbt för att börja bygga förmåga och etablera en säkerhetskultur.

4.4 Kommun



Tabellreferenser: 16, 19, 24, 26

4.4.1 NIS2 ur ett kommunperspektiv

Den kommunala verksamheten i Sverige är omfattande med sina 290 kommuner och 900 000 anställda. Digitalisering av den kommunala verksamheten har länge varit ett viktigt verktyg för att effektivisera processer och förbättra tillgängligheten för medborgarna. Variationen i storlek och förutsättningar mellan kommunerna medför att det råder stora skillnader i hur långt respektive kommun har kommit på digitaliseringsresan och detsamma gäller även för cybersäkerhetsområdet. Den generella cybersäkerhetsförmågan uppskattas vara relativt låg bland kommunerna och det kommer att krävas ett omfattande arbete för att efterleva kraven från NIS2-direktivet.

”Fram tills nu har digitaliseringen av kommunal verksamhet främst handlat om att komplettera befintliga verksamhetsprocesser och rutiner. Med kommande välfärdsbehov kopplat till pensionsavgångar och åldrande befolkning måste digitaliseringen bidra till mer transformativa förändringar och effektiviseringar. Behovet av säker digitalisering kommer vara stort.”

Kommunerna upplever ännu en otydlig situation gällande tillämpningen NIS2-direktivet. Frågan gäller om endast de samhällskritiska funktionerna (vatten, avlopp, energi med mera) kommer att omfattas av NIS2, eller om hela den kommunala verksamheten skall beröras av direktivet. Detta är en av frågorna som den statliga offentliga utredningen skall besvara, men det finns goda skäl att påbörja ett arbete med att höja cybersäkerhetsförmågan oavsett för att skydda verksamheten och inte stå helt oförberedd när resultatet av utredningen presenteras.

”Stalltipset är att NIS2-direktivet kommer beröra kommuners breda verksamhet. Och det är enligt min åsikt bra, då kommuner skulle slippa hantera sina gemensamma tjänstelager separat utifrån olika säkerhetsperspektiv.”

När det kommer till vanan runt att hantera andra regulatoriska krav så är det främst GDPR och Schrems II-domen, men till viss del även säkerhetsskyddslagen som kommuner har arbetat med. Erfarenheter från arbetet med dessa kan nyttjas som en utgångspunkt vid en NIS2-implementering.

4.4.2 Utmaningar och hot

Hotbilden mot kommuner är som tidigare nämnt ökande och riskerar att få stora konsekvenser för vår välfärd och samhällsutveckling. En stor utmaning inom denna sektor är att det råder stor variation i digital mognad, samt vilka resurser och förmågor kommunerna har för att hantera cybersäkerhet. Många kommuner kämpar med spets före bredd när det kommer till digitalisering och det råder ofta ett stort personberoende. Det kan hända att en del av verksamheten bygger ett högt kunnande och finner en best practice på bekostnad av att andra delar av verksamheten blir mer stillastående och hamnar på efterkälken.

Givet det osäkra geopolitiska läget och den ökade hotbilden påbörjar nu många kommuner ett arbete kring att bygga upp säkerhetsförmågan från en relativt låg nivå. Det grundar sig i många fall på enstaka individers engagemang, initiativförmåga och kunskap av runt cybersäkerhet (främst inom teknisk säkerhet) och efterlevnad av lagar, förordningar och ramverk. Många kommuner saknar däremot egen personal med expertis inom detta område och cybersäkerhetsexperter är både dyra och svåra att få tag på givet den stora brist på denna kompetens som råder. Detta blir särskilt utmanande för mindre kommuner att hantera.

”Ur ett kommunalt perspektiv kommer utmaningen med att öka den nationella cybersäkerhetförmågan ligga hos de minsta kommunerna. De 220 minsta kommunerna.”

Att bygga en holistisk cybersäkerhetsförmåga som innefattar perspektiven människa, verksamhet och teknik kommer att kräva moderniseringar och investeringar i teknik och insatser i utbildning och kulturuppbyggnad. Cybersäkerhetsarbetet måste ha en strategisk grund och kopplas samman med det övriga arbetet så det inte blir ett isolerat initiativ som drivs utan förankring i resten av verksamheten. Det är viktigt att ledningen tar det yttersta ansvaret för att bygga upp och underhålla förmågan ute i verksamheterna. Sammantaget kommer detta arbete kommer att kräva insatser och resurser över tid och blir då en ny ekonomisk utmaning för kommunerna.

Ytterligare en utmaning för denna sektor är bredden på den kommunala verksamheten och hur NIS2-direktivet skall kunna tillämpas på ett enhetligt sätt. För den kommunala verksamhet som uttalat kommer att omfattas (såsom vatten, avlopp, avfall, energi) ligger dessa områden inom olika utpekade sektorer med olika tillsynsmyndigheter. Det innebär att en enskild kommun kan behöva hantera tillsyn från olika myndigheter som kan ha olika rutiner och processer utifrån hur de arbetar mot respektive sektor. Sedan tillkommer även den samlade kommunala verksamheten som kanske eller kanske inte kommer att omfattas fullt ut av direktivet som då ska hanteras genom ytterligare en tillsynsmyndighet. Detta riskerar att bli en administrativ börda för kommunerna och kan bidra till att skapa en osäkerhet kring hur de bör arbeta med direktivet.

4.4.3 Mognadsgrad

Den genomsnittliga kommunen har en god mognad och vana vad gäller informationsklassning av kommunens olika datakällor. Införandet av GDPR har hjälpt till att bygga insikt och kultur brett i verksamheten kring dataskydd och dataintegritet. För att få till stånd en fullgod cybersäkerhetskultur är det inte tillräckligt, men en grund att bygga vidare på för att höja förmågan och kunskapsnivån ytterligare inom de områden som NIS2-direktivet omfattar.

Många kommuner har påbörjat ett arbete kring att förbättra cybersäkerheten och introducera nya säkerhetsåtgärder. I detta arbete bedöms införandet av regulatoriska krav som något positivt som understödjer digitaliseringsresan genom att nödvändiga investeringar och moderniseringar av IT-landskapet enklare godkänns och prioriteras.

Även i kommuners upphandlingsprocesser finns det en hög mognadsgrad vad gäller kravställning och efterlevnad av olika ramverk. Mest troligt kommer cybersäkerhet att omfattas i kravställningen i allt högre omfattning framöver och kan hanteras inom befintlig process. Det nya leverantörsansvaret inom NIS2 ställer dock nya krav på de upphandlande enheterna som behöver etablera riktlinjer kring utvärdering och riskanalys av leverantörer i linje med direktivet.

Samverkan är en viktig komponent i arbetet med NIS2-direktivet. Ett effektivt samarbete kommer att krävas mellan aktörer inom olika sektorer, gentemot myndigheter och även inom leverantörs-landskapet. Detta är ett område som kommuner generellt sett har kommit långt inom. På olika håll finns en mängd goda exempel på kommuner som har gått samman för att lösa gemensamma problem på mer effektiva sätt. Detta tillvägagångssätt kan med fördel användas i arbetet med att höja cybersäkerhetsförmågan.

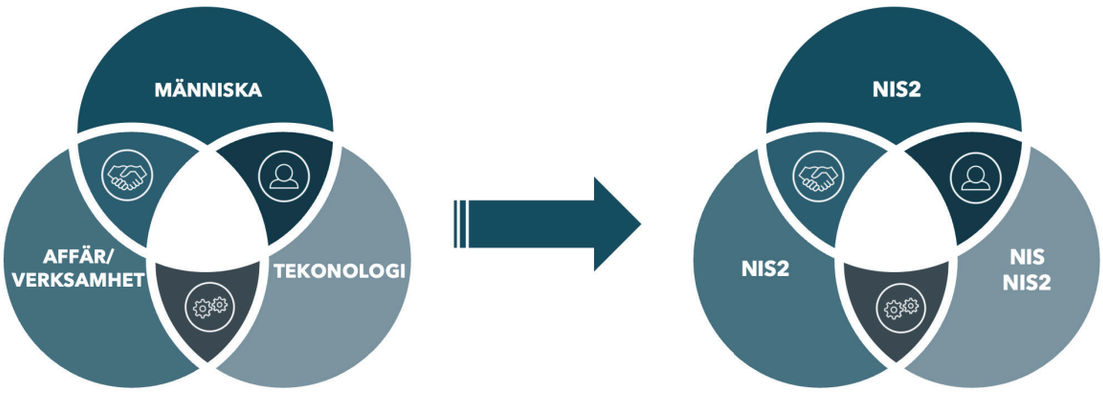
4.4.4 Call to action

1	**Kommunstyrelsen** Aktivera och bygg insikt inom kommunstyrelsen omgående för att säkra att cybersäkerheten får prioritet, resurser och mandat för att snabbt påbörja arbetet.
2	**Samverkan** Dela erfarenheter, kompetens och best practice för att effektivisera arbetet snarare än att uppfinna hjulet inom varje kommun. Detta är extra viktigt för de mindre kommunerna som ofta har få eller ingen egen personal med cybersäkerhetskompetens.
3	**Håll er uppdaterade** Var medveten om att omfattningen av kommuner inom NIS2 är under utredning. Det är viktigt att påbörja kartläggning och att bygga momentum tillsammans med verksamheten redan nu, men se till att ha ett flexibelt förfarande för att kunna anpassa till den uppdaterade kommunversionen av NIS2 när den kommer.

5. Vad bör man göra nu?

5.1 Det holistiska perspektivet

Till skillnad från många andra regulatoriska ramverk fokuserar NIS2 på att bygga upp en bred robusthet i samhället. För att uppnå detta har NIS2 ett större fokus på ledning och styrning av cybersäkerhetsarbetet och det kommer inte att räcka med att implementera tekniska lösningar för att efterleva kraven. Hela verksamheten berörs av NIS2 och efterlevnaden kommer vara avhängig verksamhetens samlande kompetens inom cybersäkerhetsområdet. Det kommer därför vara viktigt att ha ett holistiskt perspektiv på implementeringen av NIS2, där lika stort fokus läggs på de tre dimensionerna – människa, affär och teknik.



Människa – Utbildningsinsatser inom cybersäkerhet kommer att krävas av såväl icke IT-personal som medlemmar av de styrande organen för att höja hela verksamhetens försvarsförmåga och proaktivt motverka sårbarheter. Det kommer även vara viktigt att bygga insikt om påverkan på leverantörsval och att etablera processer för kravställning och uppföljning av dessa. Även i kunddialoger kommer det vara viktigt att förstå de nya ansvarsrollerna inom ramen för NIS2. En framgångsrik implementering av NIS2 kommer vara beroende av hur väl verksamheten lyckas bygga en kultur kring cybersäkerhet, med en effektiv ledning och styrning av de krav och åtgärder som direktivet föreskriver.

Affär/verksamhet – Ur ett verksamhetsperspektiv krävs en ökad visibilitet om vilka typer av affärer som görs med vilken typ av kund och vilka krav som ställs ur ett NIS2-perspektiv. En leverantör till en verksamhet som träffas av direktivet omfattas själv genom de nya leverantörskraven. Leverantören förväntas agera mer proaktivt och identifiera risker i logistikkedjan och sedan arbeta för att minska dessa. För myndigheter eller andra offentliga verksamheter som saknar kundbegreppet är grundprincipen densamma men översatt i den offentliga verksamhetens värdekedja. De ökade säkerhetskraven inom värdekedjan kan bidra till att fördjupa relationer mellan olika parter och en säker gemensam grund skapar bra förutsättningar för att bygga ett tillitsfullt och effektivt samarbete.

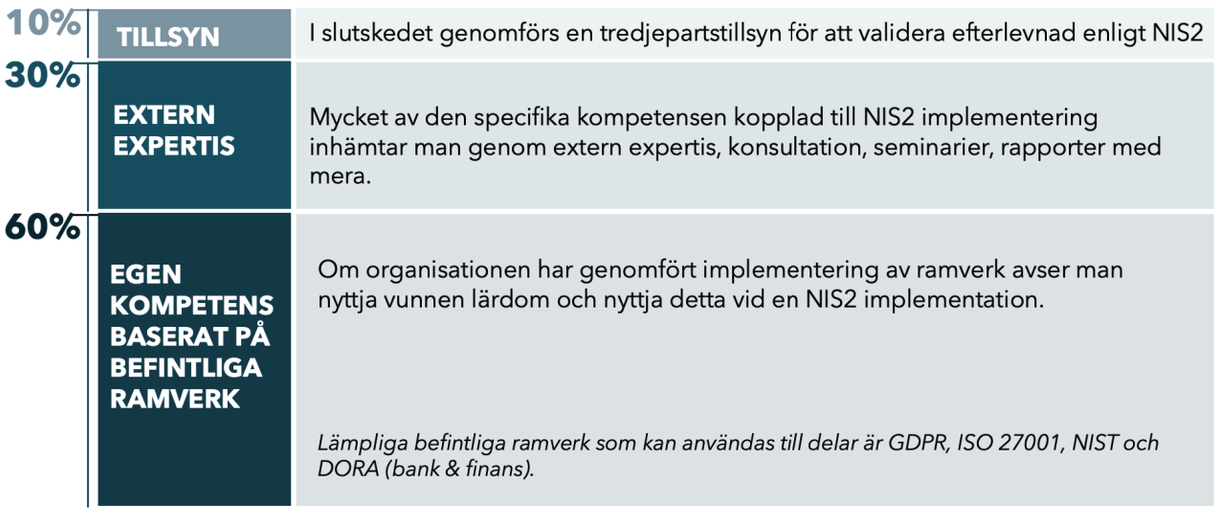
Teknik – För att hantera det ökade hotet och säkra digitaliseringen i verksamheten finns det ett behov av ytterligare modernisering, automation och dokumentation. Utöver de specifika tekniska kraven som NIS2 påbjuder sker det stora förändringar inom tekniklandskapet som kommer att skapa nya möjligheter inom cybersäkerhet, bland annat övervakningsfunktionalitet, automatisering för att underlätta rapportering samt systemstöd för dokumentation och visualisering. Ny teknik möjliggör för nya, mer avancerade metoder för att förebygga och hantera incidenter och är en del av det säkerhets-höjande arbetet.

5.2 Angreppsätt för att implementera NIS2

Arbetet med att implementera NIS2 kan vara olika omfattande eller komplext beroende på verksamhetens förutsättningar. Verksamheten kan ha olika förmågor och relationer baserat på tidigare implementeringar av lagar, förordningar eller ramverk vilket kan underlätta arbetet med nya regulatoriska krav. Vissa förutsättningar skapar ett mer omfattande implementeringsarbete medan andra underlättar kraftigt:

Enklare implementation	Mer komplex implementation
NIS (version 1) redan implementerad	Verksam på flera marknader (inom och utanför EU)
Hög mognad och efterlevnad av GDPR och/eller ISO 27001	Låg mognadsgrad kring regulatoriska ramverk
Andra implementerade regulatoriska ramverk	Verksamhet med hög andel operativ teknik (OT)
Hög insikt och förmåga hos ledningen	Verksamhet med omfattande datamängd via uppkopplade enheter (IoT)
Stark intern kultur kring cybersäkerhet	Verksamheter med omfattande leverantörslandskap
Verksam i en industrisektor med stor vana vid regulatoriska ramverk och tillsynsprocesser	

Om verksamheten har implementerat tidigare ramverk finns goda möjlig-heter att det går att dra nytta av det arbetet vid implementeringen av NIS2. I den kvalitativa research som är genomförd vid framtagandet av denna rapport angav IT-beslutsfattarna följande schematiska tillvägagångsätt och källor för nödvändig kunskap:



Många verksamheter arbetar redan aktivt med regelverk som GDPR och ISO 27001, och erfarenheten och kunskapen från arbetet med dessa kan bidra till att accelerera arbetet med att uppnå efterlevnad av NIS2. Medan GDPR fokuserar på att skydda individers integritetsrättigheter inom EU, talar ISO 27001 om att tillhandahålla åtgärder för att kontinuerligt förbättra en organisations ledningssystem för informationssäkerhet. Således ger efterlevnad av GDPR och ISO27001 en stark etablerad grund med erkänd praxis, kontroller och processer för verksamheter att bygga vidare på. Det är dock viktigt att komma ihåg att specifika åtgärder fortfarande behöver vidtas för att uppfylla samtliga krav för NIS2. Det är även viktigt att säker-ställa att verksamheten faktiskt uppnår en fullgod efterlevnad av befintliga ramverk så att grunden att bygga vidare på faktiskt är robust.

Generell best practice

Eftersom NIS2 berör nya verksamheter, sektorer och kopplar in ett tydligare leverantörsansvar än tidigare kommer det för många verksamheter bli bland de första gångerna de implementerar ett sådant ramverk. Komplexitet, omfattning och erforderlig insats för att implementera NIS2 kan därför vara svårt att överblicka. Det kan även vara så att verksamheten vid en första anblick inte bedöms omfattas, men att NIS2 ändå blir aktuellt på grund av en affärs- eller leverantörsrelation .

Därför finns det en generell best practice att anta för att snabbt få en överblick och godare beslutsunderlag:

STEG 0	**AKTIVERA**	Aktivera ledning, jurist, inköp, och IT i syfte att skapa insikt om NIS2, dess omfattning och tidsaspekten.
STEG 1	**KARTLÄGG**	Genomför en kartläggning av egen verksamhet, kunder och leverantörer med avsikt att förstå var NIS2-kraven kommer att träffa.
STEG 2	**KONSEKVENSANALYS**	Efter genomförd kartläggning tas en konsekvensanalys fram som innefattar NIS2-krav, organisationens befintliga status och behov.
STEG 3	**BESLUT**	NIS2 kommer vara en strategisk fråga som måste kopplas och förankras samt följas upp av den exekutiva ledningen.
STEG 4	**DEFINIERA IT-SYSTEM**	Skapa en tydlig bild av vilka IT-system och datakällor som berörs, och utvärdera påverkan på arkitektur.
STEG 5	**IMPLEMENTERA LEDNINGSSYSTEM**	Skapa ett riskbaserat ledningssystem med relevanta KPI: er. Dessa KPI: er behöver beröra: a) IT och data, b) operationella och c) organisatoriska aspekter.
STEG 6	**DOKUMENTERA**	Säkerhetsställ att fullgod NIS2-dokumentation upprättas och uppdateras.
STEG 7	**REVIDERA**	Genomför en tredjepartsrevision för att få en uppfattning om hur väl verksamheten efterlever kraven innan en skarp tillsyn kan bli aktuell.

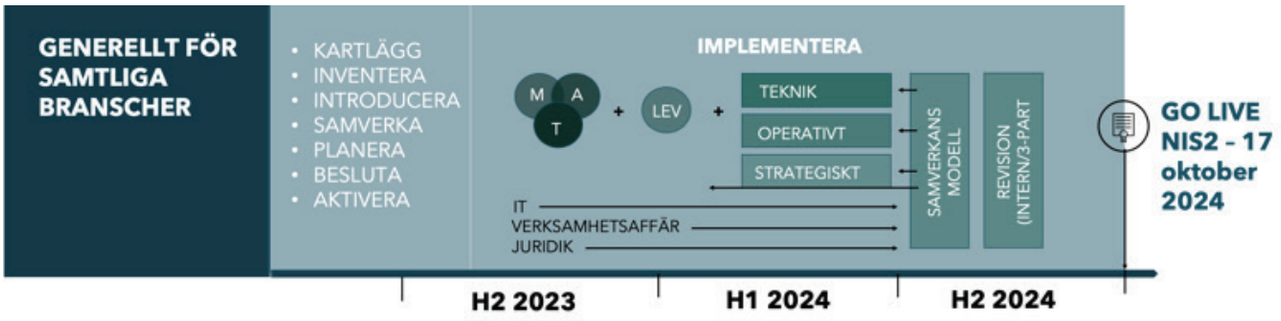
För de sektorer som utöver NIS2 även träffas av CER-direktivet så är det en god idé att samordna arbetet med implementeringen av båda direktiven som dessutom följer samma tidslinje och träder i kraft samtidigt. Många delar kan koordineras för att effektivisera arbetet såsom riskanalys, kartläggning, utbildning och etablering av interna processer för ledning och styrning. Därtill bedöms fördelarna med NIS2 stärkas ytterligare om arbetet för att säkra informations- och cybersäkerhet går hand i hand med kraven på verksamhet och kontinuitet i enlighet med CER-direktivet.

5.3 Vad ska göras när – tidslinje för implementering av NIS2

Det viktigaste rådet, som berör alla verksamheter inom alla olika sektorer, är att börja i tid. Initialt behöver verksamheten läsa in sig på kraven som ställs i NIS2-direktivet för att sedan göra en bred kartläggning av verksamheten, vilka områden som berörs, hur förutsättningarna ser ut för att uppnå kraven och eventuella gap som kräver insatser.

I nästa fas påbörjas arbetet med att implementera direktivet i verksamheten. Det är av yttersta vikt att ledningen är engagerad i arbetet från start och att det finns en strategisk förankring i allt som görs. Därtill är det viktigt att bibehålla ett holistiskt perspektiv i de tre dimensionerna människa, affär/verksamhet och teknik. Lika viktigt som det är att introducera nödvändiga tekniska säkerhetslösningar i verksamheten är det att säkerställa att det finns processer, strategiskt stöd och nödvändig kompetens runt dessa för att lösningen skall få önskad effekt och skapa nytta. Det är även viktigt att tidigt börja arbeta med leverantörslandskapet, både i en inledande inventering och kravställning, men även för att diskutera former för fortsatt samverkan.

Nedan följer en schematisk uppställning av de aktiviteter som verksamheten behöver genomföra innan NIS2 träder i kraft.

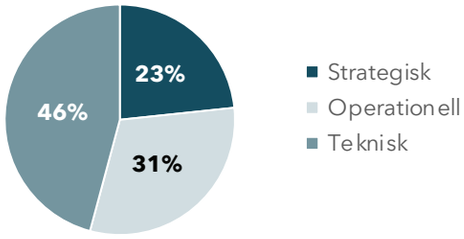


5.4 Kostnader och investeringar för att implementera NIS2

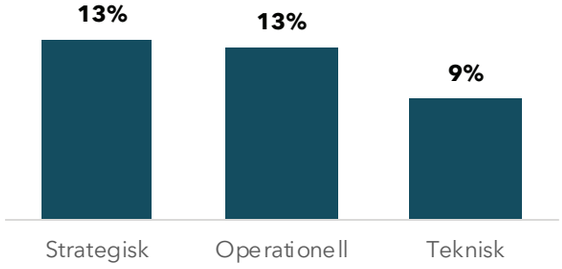
Den samlade europeiska budgeten för informationssäkerhet uppgår till strax under 7 procent av den totala IT-budgeten för 2022. Det är anmärkningsvärt nog en minskning med en procentenhet från föregående år. Det är en ogynnsam utveckling med den rådande geopolitiska utvecklingen och stämmer inte överens med den politiska ambitionen.

Enligt Radars analys lägger Sverige en samlad budget av 5,8 procent på cybersäkerhet, motsvarande 13,4 miljarder SEK under 2023[21]. Till skillnad från den europeiska avmattande trenden ökar budgeten för cybersäkerhet i Sverige, där tillväxttakten är störst inom strategisk och operationell säkerhet och där teknisk säkerhet fortfarande utgör den största andelen, men har den lägsta tillväxttakten.

Fördelning av svensk cybersäkerhetsmarknad[21]



Estimerad tillväxt 2023[21]



I definitionen av teknisk cybersäkerhet ingår teknik, såsom verktyg, applikationssäkerhet och övervakning. Inom operationell cybersäkerhet återfinns kostnader och investeringar kopplade till tjänster inom cybersäkerhetsområdet, som exempelvis information, underrättelse och incidentrespons. Strategisk cybersäkerhet är kopplad till att bibehålla den strategiska förmågan över tid, med exempelvis konvergens, regulatorisk efterlevnad, strategiska överväganden och digital affärsriskhantering[21].

Fördelningsprioriteringen stämmer väl överens med de nytillkomna delar som NIS2 adresserar jämfört med det ursprungliga NIS-direktivet som var av mer teknisk och operativ karaktär. NIS2 har ett mycket högre fokus på rapportering, utbildning och samverkan samt proaktiv riskhantering inom både den egna verksamheten samt i ens leverantörsled.

NIS2 driver ökade kostnader

Att implementera NIS2-direktivet kommer att kräva investeringar. Hur stora de blir är beroende på hur komplext och omfattande arbetet blir för verksamheten samt vilket tillvägagångssätt som verksamheten väljer. Det är viktigt att denna kostnad tas i beaktande tidigt inom relevanta budgetar för att inte riskera att sakta ner arbetet. Europeiska kommissionen presenterar följande nyckeltal att utgå ifrån:

Uppskattad kostnad för att implementera NIS2[2]	
Befintlig NIS-verksamhet	**Inte träffad av NIS (version 1)**
+12%	**+22%**
Ökad kostnad inom informationssäkerhets-budgeten de kommande 3 åren	**Ökad kostnad inom informationssäkerhets-budgeten de kommande 3 åren**

Tabellen nedan visar en skattningsfördelning av verksamhetens troliga kostnadsökningar för att implementera NIS2 inom olika områden. Den uppskattade kostnadsfördelningen skall enbart ses som just en uppskattad kostnadsfördelning och inte en prioriteringsordning, det vill säga var det krävs mest insatser eller vilken del som är mest kritisk för efterlevnad av NIS2.

UPPSKATTAD FÖRDELNING AV NIS2-KOSTNADER[2]), Implementering över 3år			
Applikationssäkerhet	+++	Identitet och access	++
Molnsäkerhet	+++	Infrastruktur	++
Data & integritet	++(+)	Riskhantering	+

6. Vilka förmågor krävs i framtiden

I detta kapitel knyts rapportens inledning om Sveriges digitala motor och behovet av fortsatt digitalisering ihop med Ciscos syn på framtida behov och förmågor för säker digitalisering. Vidare delar Cisco med sig av ett konceptuellt tänk och best practice kring att bygga verksamhetens framtida cybersäkerhetsförmåga. Diskussionen i detta kapitel bygger på ett generellt cybersäkerhets-perspektiv men är även anpassat för ett förestående implementationsarbete av NIS2-direktivet.

6.1 Ciscos värdeskapande i det transformativa cyberlandskapet

Ciscos ambition är att bidra till att stärka den digitala ekonomin och det digitala samhället med best practice för säker digitalisering. Ett exempel är det globala samarbetsinitiativet ”Cisco Country Digital Acceleration Program” (CDA) med över 1 500 pågående digitala initiativ i över 48 länder. Nedan är exempel på initiativ under Ciscos CDA-program som bidrar till en säker digitalisering och på så sätt bistå EU i sin ambition att säkra den digitala ekonomin och det digitala samhället:

- Cisco har tillsammans med EU kommit överens om att utbilda 250 000 EU-medborgare i digital kunskap och cybersäkerhet de kommande 3 åren.
- Tillsammans med kunskapsbärande myndigheter har Cisco utbildat 50 generaldirektörer och dess ledningsgrupper i cybersäkerhet.
- Cisco genomför ett nationellt initiativ tillsammans med kommuner att modernisera skolors nätverk.

Dessa initiativ bidrar till att stärka utvecklingen inom området humankapital genom att fokusera på att höja kompetensnivån och stärka den digitala förmågan, både på bredden inom EU men även i ett riktat initiativ mot svenska generaldirektörer. NIS2-direktivet slår fast att det är kritiskt att ledningen aktiveras och utbildas inom cybersäkerhet för att kunna driva och skapa förutsättningar för nödvändig förändring inom verksamheter. Detta initiativ bidrar tydligt till det arbetet. Därtill stärker Ciscos arbete med att modernisera skolors nätverk den svenska förmågan inom området konnektivitet och skapar förutsättningar för digitala offentliga tjänster.

En konceptualisering av säker digitalisering

Ytterligare ett exempel på hur Cisco nyttjar sina förmågor för att bidra till en säker digitalisering är framtagandet av en värdeskapande strategi som bygger på tre koncept: konnektivitet, automatisering och säkerhet.

- **Konnektivitet**: Möjliggör för verksamheten att snabbt anpassa sig till framtida arbetssätt. Inkluderar både traditionell IT (IT) och operativ IT (OT).
- **Automation**: Förenklar driften med agila automatiserade tjänster, funktioner och plattformar.
- **Säkerhet**: Integrerad säkerhet för alla lösningar, alla användare och all data.

Under 2022 kunde Cisco, genom att nyttja detta koncept med en datadriven automatisering, expertis inom cybersäkerhet och sin etablerade förmåga runt konnektivitet globalt avvärja en kvarts miljard cyberhot per dag. En fördel med detta koncept är skalbarheten som möjliggör att det kan implementeras i det lilla sammanhanget likväl som i det större sammanhanget i både privata och offentliga verksamheter.

”Vi har en långvarig relation med Cisco, men med Ciscos konceptuella tänk runt säker digitalisering lyckades vi lyfta cybersäkerhetsfrågan till att bli en gemensam bolagsfråga tillsammans med ledningen.”

Konnektivitet

Sammankopplingen av användare med applikationer och data utgör grunden för digitaliseringen av samhället som har skapat fantastiska möjligheter men också bidragit till en ökad komplexitet. Cisco har en lång erfarenhet av att knyta samman människor med utrustning, applikationer och data tillsammans med världsledande nätverks- och datacenterteknologi för att möjliggöra samarbete och värdeskapande i verksamheter och samhället i stort. Denna uppkoppling är grunden till det moderna hybrida arbetssättet, men för att fortsatt åtnjuta fördelarna med digitaliseringen måste ett ökat fokus läggas även på automatisering och säkerhet.

Automatisering

Automation är nyckeln till att binda samman säkerhet och infrastruktur för att kunna skapa en mer säker och flexibel IT-miljö, utan att behovet av resurser och specialistkompetens ökar. I och med digitaliseringen har vi skapat digitala verktyg och system som skapar mer effektiva processer och nya grunder för värdeskapande. Genom att integrera de olika systemen skapas en ökad visibilitet och tiden för att upptäcka och åtgärda hot minskas. Automatisering möjliggör nya sätt att fånga och nyttja potentialen från den genomförda digitaliseringen.

En genomgående utmaning är en stor brist på kompetens och personal inom IT-säkerhet, vilket gör det svårare för verksamheter att effektivt integrera cybersäkerhet i digitaliseringsarbetet. Cisco adresserar detta behov genom att erbjuda en hög grad av automatisering, inklusive prediktiv AI, i sina lösningar.

Säkerhet

Ett stort fokus har länge legat på de första två delarna, men för att säkra den redan genomförda digitaliseringen samt skapa förutsättningar för nästa steg av värdeskapande med hjälp av automatisering måste cybersäkerhet få ett större fokus. Det handlar om att säkra alla användare, all utrustning

och alla applikationer överallt. Grunden för säkerhetsarbetet är en systematisk säkerhetsanalys och en säkerhetsplan som har en strategisk förankring i verksamheten och ledningens stöd.

Några av baskraven för att uppnå en säker IT-infrastruktur är autentisering, segmentering, filtrering, och visibilitet. Kravbilden är densamma oavsett om systemen ligger i molnet, hybridlösningar eller i egen miljö.

De viktigaste nyttoeffekterna med Cisco-koncepten är att kompentensen blir skalbar, snabbare upptäckt och hantering av hot och incidenter och en konsekvent policy från applikation till infrastruktur. I den dagliga verksamheten är vinsten framför allt det minskade behovet av specialistkompetens för daglig drift och rutinändringar.

6.2 Ciscos specifika förmågor för säker digitalisering

De tre koncepten, konnektivitet, automatisering och säkerhet bidrar till en säkerhetsarkitektur med integrerade säkerhetsfunktioner i det fysiska och logiska nätverket. Genom att skapa ett samspel mellan dessa funktioner minskar behovet av specialistkompetens och möjliggör även snabbare hantering av IT-incidenter till en lägre kostnad. Även kvalitén och precisionen förbättras med hjälp av automatisering samt tydliga och enhetliga policyer.

Ciscos förmågor för säker digitalisering		
KONNEKTIVITET	**Uppkopplingslösningar som bidrar till säker digitalisering:**	
	Ciscos nätverksportfölj för IT & OT Management Intent-based networking Nätverk managerade lokalt och i molnet	Internet Wide Area Networks (WAN) Access networks Data center networking Molntjänster (publik, hybrid, privat)
AUTOMATISERING	**Automatiseringstjänster som bidrar till säker digitalisering:**	
	Extended Detection and Response XDR Öppna API'er Öppen Telemetri Full-stack Observability	Time-to-detect Time-to-remediation Expertrådgivning
SÄKERHET	**Säkerhetslösningar om bidrar till säker digitalisering:**	
	Indelning av applikationer i zoner Indelning i nätverkssegment Filtrering av dataflöden Digitala identiteter Behörighetshantering Flerfaktorsautentisering Kryptering Skydd mot obehörig åtkomst och förändring Säkerhetsloggar	E-postsäkerhet Säkerhetskonfigurering Säkerhetstester och granskning Analys av säkerhetsloggar Intrångsdetektering och intrångsskydd Skydd mot skadlig kod Skydd av utrustning Redundans och återställning AI-baserade säkerhetsfunktioner Extended Detection and Response Data Loss prevention

7. Slutord

Sverige har kommit långt i den digitala utvecklingen och inom alla sektorer i samhället ses digitalisering som en strategiskt viktig komponent för framtiden. Det finns en utbredd insikt kring värdet av digitalisering, men trots det saknas på många håll kunskap och förmåga kring hur digitaliseringen kan utvecklas säkert.

Det finns en samlad potential med att digitalisera i Sverige som uppgår till mer än 800 miljarder. Samtidigt finns det en potentiell risk på mer än 70 miljarder av att genomföra en icke säker eller undermålig digitalisering. Detta utrymme på nära 900 miljarder ligger i samhällets intresse att försöka kapitalisera på för vår framtida ekonomiska utveckling och konkurrenskraft.

I takt med att samhället blir alltmer digitalt och uppkopplat ökar hotet och risken för cyberattacker. Incidenter har ökat i både antal och kostnad och sårbarheten har nått en nivå som inte bara är en belastning för den som drabbas utan för samhället i stort. EU:s breda regulatoriska ramverk NIS2 är ett politiskt svar på denna utveckling som skapar en gemensam plattform för ökat samarbete och ökad cybersäkerhetsförmåga.

NIS2-direktivet omfattar ett stort antal verksamheter i både privat och offentlig sektor. Genom en analys av olika branschers erfarenheter och insikter kring att implementera andra lagar, förordningar och ramverk har en generell best practice utkristalliserats. Börja i tid, se till att säkerhetsarbetet har en strategisk förankring i verksamheten, etablera en cybersäkerhetskultur och engagera ledningen från start. Cybersäkerhet har kommit att bli en strategisk verksamhetsfråga, men ytterst kopplas den samlade cybersäkerhetsförmågan ihop med nationens säkerhet och ekonomiska välfärd. Säker digitalisering har blivit essentiell. För alla.

Kommentarer från de intervjuade verksamheterna

”Detta är en möjlighet, där man tillsammans kan bygga upp en gemensam förmåga mellan den offentliga verksamheten och privata sektorn.”

”Det finns nu ett stort behov av snabb och samman-förande rådgivning, tolkning och förtydligande från de nationella myndigheterna, i syfte att klargöra och föra samman kommunala, regionala och privata initiativ runt NIS2-direktivet”

”Det kommer vara en fråga om tillgång på kompe-tens vid införandet av NIS2. Denna kompetens är en bristvara. Just nu finns det ett visst anorektiskt beteende där vi tar ifrån varandra. Vi som nation skulle tjäna på en gemensam nationell förmåga, som framför allt skulle kunna stötta i det kommunala perspektivet.”

”Ur ett nordiskt perspektiv finns det inspiration att hämta ifrån både Finland och Danmark, men även Norge, som alla har använt ett mer centrali-serat styrande perspektiv vid införandet av breda ramverk och förordningar. Det hjälper dem att komma snabbare ur startblocken och skapa en bred samsyn snabbt.”

8. Referenslista

1. DNV AS (2023). NIS2 Directive: Compliance risk or cyber security opportunity? https://www.dnv.com/Publications/nis2-directive-compliance-risk-or-cyber-security-opportunity--238994
2. ENISA (2022:1). NIS investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
3. ENISA (2022:2). Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
4. European Commission (2020). Annexes 1-3 to the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive 2016/1148. https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_2&format=PDF
5. European Commission (2023). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
6. European Parliamentary Research Service (EPRS) (2023). The NIS2 Directive: A high common level of cybersecurity in the EU. The 'EU Legislation in Progress' briefing 2023-02-08. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
7. European Union [EU] (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684142672664
8. European Commission (2023). The Digital Economy and society index (DESI) 2022. https://digital-strategy.ec.europa.eu/en/policies/desi
9. WIPO Global Innovation Index (2023). Global Innovation Index Report 2022. https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf
10. Startup Ranking. Startup Ranking 2023. https://www.startupranking.com/countries
11. Finansinspektionen (2022). Förstärkt digital motståndskraft hos företag i den finansiella sektorn. https://www.fi.se/contentassets/7ed22f2de362421b8590699ec253746e/forst-digital-motstndskraft-ftg-fin-sektor.pdf
12. FRA (2022). Årsrapport 2022. Året då kriget kom till Europa. https://fra.se/download/18.54ed4de-8186313dc3566d/1678969166868/FRA-arsrapport-2022_TGA_Enkel.pdf
13. Harvard Business Review (2017). What the companies on the right side of the digital business divide have in common. https://store.hbr.org/product/what-the-companies-on-the-right-side-of-the-digital-business-divide-have-in-common/H03ED2
14. Harvard Business Review (HBR) (2023). What Business Needs to Know About the New U.S. Cybersecurity Strategy. https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy?ab=hero-subleft-1
15. iCore (2023). Affärsnyttan med ett moget data- och integrationsarbete. https://www.icoresolutions.com/sv/blogg/white-papers/affarsnyttan-med-data-och-integrationsarbete
16. McKinsey (2017). Möjligheter för Sverige i digitaliseringens spår. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/europe/mojligheter%20for%20sverige%20i%20digitaliseringens%20spar/digitizing-sweden-mojligheter-for-sverige-i-digitaliseringens-spar.ashx

17. McKinsey (2020). How COVID-19 has pushed companies over the technology tipping point – and transformed business forever. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/How%20COVID%2019%20has%20pushed%20companies%20over%20the%20technology%20tipping%20point%20and%20transformed%20business%20forever/How-COVID-19-has-pushed-companies-over-the%20technology%20tipping-point-final.pdf

18. MSB (2022:1). När kriget kom nära. Årsrapport IT-incidentrapportering 2022. https://rib.msb.se/filer/pdf/30339.pdf

19. MSB (2022:2). Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. https://rib.msb.se/filer/pdf/30002.pdf

20. Radar (2021). Från IT-säkerhet till digital affärsrisk. https://hub.radargrp.com/reports

21. Radar (2023:1). Cybersäkerhet 2023 – i ett alltmer osäkert och utsatt läge. https://hub.radargrp.com/content/svensk-cybersakerhet-2023

22. Radar (2023:2). IT Radar 2023. https://hub.radargrp.com/content/it-radar-2023

23. Regeringen (2023). Kommittédirektiv: Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. https://www.regeringen.se/contentassets/77a6664e7064451c8616caef98fd6961/genomforande-av-eus-direktiv-om-atgarder-for-en-hog-gemensam-cybersakerhetsniva-i-hela-unionen-och-eus-direktiv-om-kritiska-entiteters-motstandskraft.pdf

24. SCB (2022). Sveriges BNP. [2023-06-09]. https://www.scb.se/hitta-statistik/sverige-i-siffror/samhallets-ekonomi/bnp-i-sverige/

25. Svenska Bankföreningen (2023). Svensk Bank och Finansstatistik 2022 [2023-05-31]. https://www.swedishbankers.se/fakta-och-rapporter/statistik-och-rapporter/bank-och-finansstatistik/

26. Sveriges Kommuner och Regioner (2023). Statistik [2023-06-12]. https://skr.se/skr/tjanster/statistik.46562.html

27. Säkerhetspolisen (2022). Säkerhetspolisen 2022–2023. https://www.sakerhetspolisen.se/download/18.36cda2851868025da5b2b/1677241538918/SP_Årsbok_2022__Anpassad.pdf

28. Truesec (2023). Treat Intelligence Report 2023. An In-Depth Analysis of the Cyber Threat Landscape. https://www.truesec.com/hub/report/threat-intelligence-report-2023

29. US government (2023). US National Cybersecurity Strategy (2023). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

30. Centre of Cyber Security (CCB) (2023). NIS2: Where are you? https://ccb.belgium.be/en/news/nis-2-where-are-you

31. EUR-Lex (2023). Commission Staff Working Document Impact Assessment Report. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345

32. MSB (2023). Infosäkkollen (2021). https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/

33. SCB (2023). Sveriges framtida befolkning 2017–2070: Störst folkökning att vänta bland de äldsta. https://www.scb.se/hitta-statistik/statistik-efter-amne/befolkning/befolkningsframskrivningar/befolkningsframskrivningar/pong/statistiknyhet/sveriges-framtida-befolking-20182070/

34. European Commission. Shaping Europe's digital future (2023). Final Study Report: The European Data Market Monitoring Tool. https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure

9. Bilagor

Bilaga A: Det regulatoriska landskapet

2016–2019	2020–2021	2022–2023
Integritet & dataskydd	**Digital suveränitet**	**Regulatoriska ramverk**
GDPR US Cloud Act Schrems II	EU Strategy for Data	EU–US Data Privacy Framework EU Data Act EU AI Act EU Cybersecurity Act ENSIA Cloud Security Certification NIST Cybersecurity Framework CER-direktivet DORA-förordningen

Integritet & dataskydd (2016–2019)	**GDPR**	Införandet av den allmänna dataskyddsförordningen (GDPR) trädde i kraft år 2018 och markerade starten på den mest strikta integritets- och säkerhetslagstiftningen i världen. Denna förordning sätter en helt ny standard för dataskyddsbestämmelser och lagar.
	US Cloud Act	EU-baserade företag som använder en amerikansk molnleverantör för att lagra eller hantera sin data juridiskt kan vara skyldiga att dela denna data med amerikanska myndigheter i händelse av en utredning av allvarliga brott.
	Schrems II	Reglerar säker överföring av personuppgifter från EU till USA. Genom denna lagstiftning har sättet som företag och lagstiftare hanterar dataöverföringar och respekterar användarnas integritet förändrats på ett oåterkalleligt sätt.
Digital suveränitet (2020–2021)	**EU Strategy for Data**	EU:s digitala strategi omfattar flera akter: Data Governance Act skapar ett nytt sätt att hantera data för att öka förtroendet för och underlätta datadelning. Digital Markets Act skapar rättvisa och omtvistade marknader för innovation, tillväxt och konkurrenskraft i den digitala sektorn.
Regulatoriska ramverk (2022–2023)	**EU–US Data Privacy Framework**	Data Privacy Framework kommer att träda i kraft före sommaren 2023 och avser att säkerställa att känsliga och kritiska data skyddas för att förbättra digital suveränitet för organisationer i Europa och över hela världen.
	EU Data Act	EU:s Data Act säkerställer rättvisa genom att tillhandahålla regler om användningen av data som genereras av Internet of Things (IoT) – enheter.
	EU AI Act	Spridningen av data och det ökade antalet nya AI-system gett upphov till denna reglering. Målet med AI-lagen, som förväntas slutföras i år, är att reglera AI-tillämpningar och anpassa dem till EU:s övergripande värderingar och grundläggande rättigheter.
	EU Cybersecurity Act	Med de senaste årens ökande cybersäkerhetshot har EU lanserat flera förordningar och initiativ för att skydda medborgare och organisationernas säkerhet och integritet. En sådan lag är EU Cybersercurity Act som ökar det operativa samarbetet på EU-nivå i fall av storskaliga gränsöverskridande cyberattacker och kriser.
	ENISA Cloud Security Certification	ENISA bidrar till EU:s cyberpolicy, förbättrar tillförlitligheten hos IKT-produkter, tjänster och processer med cybersäkerhetscertifiering.
	NIST Cybersecurity Framework	NIST hjälper företag av alla storlekar att bättre förstå, hantera och minska sin cybersäkerhetsrisk och skydda deras nätverk och data. Ramverket är frivilligt.
	CER-direktivet	CER-direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.
	DORA-förordningen	DORA-förordningen syftar att bidra med en ökad digital operativ motståndskraft inom EU:s finanssektor. Det avser implementering av policys, verktyg och ramverk för riskhantering, rapportering och testning i avsikt att minimera risken och eventuella följder vid IKT-relaterade incidenter.


CISCO